From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974

ROBERT GELLMAN PRIVACY ACT PROJECT

APRIL 2021

WORLD **PRIVACY** FORUM

From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974

5 U.S.C. § 552a

PRIVACY ACT PROJECT

April 19, 2021
Version 2.01a

ROBERT GELLMAN
Privacy and Information Policy Consultant
419 Fifth Street SE
Washington, DC 20003

202-543-7923
bob@bobgellman.com
www.bobgellman.com

Contents

Executive Summary

The goal of the Privacy Act Project is to revise, update, and replace the Privacy Act of 1974. The title of the proposed revision is the *United States Agency Fair Information Practices Act* (USA FIPS Act). This report explains the original Privacy Act, some of its history, and why the current law out-of-date.

The objectives of the Privacy Act Project are to:

1. Bring the Privacy Act of 1974 up to date in recognition of current approaches to privacy protection, modern personally identifiable information processing activities, and new information technologies.
2. Preserve the individual rights in existing law and make it easier for individuals to exercise those rights.
3. Allow agencies to implement their responsibilities in a more efficient and more effective way.
4. Make the new Act consistent with other relevant information management laws, while bringing most privacy-related obligations for federal agencies under one legislative framework.

*****

Part I of this report sets out some history of the Privacy Act Project and discusses the objectives of the revision.

Part II includes a brief history of the original Privacy Act of 1974 and selected oversight activities over the years.

Part III reviews several major issues with the current law that the proposed legislation seeks to reform. One of those issues is the *system of records*, a central defining feature of the law that reflects outdated conceptual models (file cabinets and mainframe computers). Even so, agency publication of descriptions of their systems of records remains a significant contribution to public understanding of agency record keeping practices. The basic concept needs to be revised and updated.

A second major feature of the Privacy Act gives agencies the ability to establish disclosures (*routine uses*) that are compatible with the purpose for which records were collected. However, this standard did not effectively limit disclosures. The problem of defining and restricting compatible disclosures is a challenge for privacy laws around the world, and no simple solution is apparent.

A third major feature of the existing law is its approach to exemptions. While the Privacy Act does not allow any secret systems of records, some systems can be exempted from some of the Act's requirements. The report identifies some shortcomings and inconsistencies in the exemptions.

Part IV offers a section-by-section discussion of the USA FIPS Act. The proposed law is more evolutionary than revolutionary. Three main changes in the proposal are:

1. Replacing *systems of records*. The USA FIPS Act proposes to replace the existing *system of records* definition that relies on how agencies actually retrieve records. The replacement is a functionally-

based concept called an *agency activity affecting privacy* (A3P). Agencies would have broad authority to decide how to group activities within A3Ps. Descriptions of A3Ps must include more information about agency use of non-governmental records.

2. Refining *routine uses*. The USA FIPS Act gives agencies the ability to define three flavors of agency *designated disclosures*, with procedural limits and requirements that are largely absent from the existing law. Because of the difficulty of establishing clear standards for distinguishing appropriate from inappropriate disclosures, the proposed law provides processes and procedures that serve to restrict the promulgation of inappropriate disclosures while still allowing agencies the ability to disclose records for their operations and as required by law.

3. Reforming the civil remedies. Supreme Court rulings limit the ability of an individual to pursue rights or find redress under the unique standards of the Privacy Act. Also, for many actions by agencies, it does not appear that public interest groups or others can readily challenge core elements such as routine uses, the scope of record systems, and procedural obligations. The USA FIPS Act modestly improves remedies for individuals and creates a new administrative remedy that allows any person to pursue complaints that an agency is not complying with the law.

In addition to these three major changes, the USA FIPS Act provides:

- rights to foreign nationals and not just citizens and resident aliens;
- continues with modest improvements current individual rights of access and amendment;
- requires each agency to have a Chief Privacy Officer with significant substantive and procedural authority;
- establishes requirements for Privacy Impact Assessment Processes;
- adjusts but largely continues existing exemptions and computer matching obligations;
- extends the scope of the law beyond agency contractors;
- establishes enhanced criminal penalties; and
- provides agencies with a long transition period to move from compliance with the Privacy Act to compliance with the USA FIPS Act.

The text of the draft bill appears in each relevant part of the section-by-section discussion. A complete copy of the draft bill appears in full in Appendix I.

Part I. The Privacy Act Project: A Personal Introduction

A. Origins of the Privacy Act Project

I started the Privacy Act Project in 2019 with the goal of redrafting the Privacy Act of 1974. While Internet and consumer privacy matters currently receive considerable public and legislative attention, the Privacy Act of 1974 is somewhat of an orphan. The Act is old, predates the Internet, and applies only to federal agencies and some federal contractors. The cutting edge of personally identifiable information processing and the focus of privacy legislation are elsewhere and have been for a long time. The Act is too narrow to be of general interest. It is no one's privacy priority. Yet as the principal privacy law for the entire federal government, the Privacy Act of 1974 remains an important law and one that needs updating.

My involvement on privacy matters began shortly after passage of the Act. In 1975, I worked in the Office of General Counsel at the General Accounting Office (now the Government Accountability Office). My boss at the time assigned me to be the agency's Privacy Act lawyer. Eventually, my experience with the Act and other information policy laws led me to join the staff of the Subcommittee on Government Information of the House Committee on Government Operations. I was the principal House staffer for the Privacy Act of 1974 as well as for the Freedom of Information Act for 17 years (1977-1994). After leaving the Hill, my consulting practice included Privacy Act work for several federal agencies that included revising systems of records notices and agency rules. This brought me a new perspective on the Act. Over the years, I also drafted comments on agency Privacy Act notices for public interest groups.

As will be clearer as you read this document, the Privacy Act received some attention in the years after its passage. The first hearing I organized as a House staffer was to receive the report of the Privacy Protection Study Commission in 1977. That report that made numerous recommendations for privacy in general and for changes to the Privacy Act in particular. None became law. While Congress made one significant change to the Act through the Computer Matching Amendments in 1988, concern about the general shortcomings of the Act remained low.

During my tenure on the Hill, there was virtually no political or policy interest in revising the Act to be found anywhere. The public started to show interest in privacy matters in the mid-1990s, in part because of the rise of identity theft and in part because of the growth of the Internet. Nevertheless, the Privacy Act of 1974 attracted little attention. As privacy grew as an international subject of regulation in the last two decades of the 20th century, the focus was largely on the Internet and on commercial activities. New national laws elsewhere generally apply to many types of personally identifiable information, including data in government agency records. Interest in a national U.S. privacy law is quite recent, and I am not aware of any current proposal that seeks to replace or change the Privacy Act of 1974. The Judicial Redress Act of 2015 gave some Privacy Act rights to foreign nationals, but the Judicial Redress Act was mostly a political demonstration for EU privacy regulators rather than a serious attempt to address existing Privacy Act shortcomings.[1]

This report is a personal project. I decided to undertake revision of the Act because no one else seemed willing to do so. I received no funding for the Privacy Act Project. The World Privacy Forum

[1] The Judicial Redress Act was a product of the House and Senate Judiciary Committees. Neither Committee has jurisdiction over the Privacy Act of 1974.

sponsored the project and provided administrative and editorial support. The Center for Democracy and Technology provided meeting space. A host of individuals, privacy advocates, former and current federal government employees, and others provided comments, offered ideas, gave critiques, attended meetings, read drafts, and assisted in other ways. The help of those interested in the Act – whom I like to call *Privacy Act Nerds* – was invaluable. Many of the ideas reflected in this report and in the bill came from or were shaped by their comments, suggestions, and responses.

However, by express agreement, the names of all who participated in any way in the Privacy Act Project are confidential. Participation in the project was a personal act, and no one officially represented the agency or organization that employed them. The promise of confidentiality allowed some to participate who could not have done so on any other basis. Everyone labored in good faith to help produce a workable bill. The final bill reflects contributions from each individual in some way. In the end, however, all the choices, judgments, and decisions are mine, and I alone take full responsibility for the bill, for any shortcomings, and for this report.

Some of the judgments made here reflect the experience with existing law; some reflect policy considerations; and some are political judgments. A wonderful bill that cannot pass only accomplishes so much. One of my goals was to prepare a bill with a reasonable chance of passage. If federal agencies express major opposition to it, the chances of passage will decrease significantly. Similarly, a revised bill has to address features of current law that privacy and consumer advocates do not like. I like to think that there is a rough balance of pluses and minuses from all perspectives. I do not expect that everyone will agree with all of the choices, and I recognize that there will be plenty of opportunity for further debate. This bill and report are just starting points for that debate.

I want to offer a comment about the title of the bill. I did not include the word *privacy* in the title. Most nations in the world address information privacy with *data protection* laws. That is a more precise description of the scope of modern information privacy laws. Unqualified, the term *privacy* could apply to a wide variety of interests as wide ranging as the practice of religion, bodily interests, personal relationships, as well as personally identifiable information. Privacy interests broadly defined vary from country to country and from culture to culture. There is much more commonality and more precision with the term *data protection* or *information privacy*.

During the 96th Congress, I worked intensively on a bill titled the *Privacy of Medical Information Act*. Like nearly all privacy laws since, the bill had a significant number of exceptions that allowed for the use of health records without individual consent. I heard repeated objections that a privacy bill should not have so many exceptions. When I asked objectors to select an exception to which they objected, I rarely had any difficulty justifying the exception to them. Yet objectors still walked away feeling that the bill did not adequately protect privacy.

In the 103rd Congress, my subcommittee tried again to enact a health privacy law. Learning from past experience, I titled the bill the *Fair Health Information Practices Act*. The bill promised Fair Information Practices (FIPs) rather than privacy, and the previous objections did not return, at least not in the same way. There were still plenty of controversial matters, but the title of the bill altered the terms of debate, at least slightly. Neither the bill from the 96th Congress nor the 103rd Congress became law.

The Privacy Act of 1974 allows for numerous nonconsensual disclosures. So does the bill proposed in this report. Privacy remains a complex matter, and one that requires compromise with other interests and values.

Understanding about information privacy increased over the past decades, with significant contributions from countries with data protection laws. Data protection remains an unfamiliar term in the United States. Fair information practices originated in the United States. Elsewhere, this report explains the history and importance of FIPs. For many reasons, therefore, the title of the proposed bill is the USA FIPS Act.

I offer an additional introductory word about this report. Writing a policy report in first person style is not common in America. British traditions support the use of first person. My inspiration came in part from the 1972 British Report of the Committee on Privacy, better known as the Younger Report, which I read for background while working on revisions to the Privacy Act. Given the process from which this report emerged, I am comfortable using the first person, but I thought it needed an explanation.

B. Scope and Objectives

The same FIPs that formed the basis for the Privacy Act of 1974 remain relevant to privacy protection today. Professor Priscilla Regan called FIPs the "components of fairness in record keeping,"[2] and fairness remains an important overall goal. Paula Bruening observed that FIPs provide a common language of privacy that provides value to all, regardless of their particular implementation of privacy principles.[3]

However, FIPs are not sufficient or detailed enough to address all current information privacy needs. FIPs need not be abandoned or superseded in favor of other privacy standards, however. FIPs remain foundational principles in privacy laws everywhere around the world. Technology, administrative developments, and a better understanding of what is needed to protect privacy add elements, ideas, and implementations that extend beyond FIPs to international privacy policy discussions, debates, standards, and laws.[4] A more recent focus on ethics suggests a recognition of the need for additional ways to make judgments about legitimate processing of personally identifiable information.[5] Many voices and perspective contribute to achieving an overall objective of fairness in processing of personal information.

It is not my goal in this report to revise or restate basic privacy principles. Much of the craft of privacy today is finding ways to implement core principles in fair and balanced ways that allow record keepers to carry out essential functions while providing appropriate protections for individuals and their data. Note the numerous "weasel words" in that last sentence. Still, a premise of this report is that we can find agreement on ways to direct federal agencies to address privacy without necessarily reaching agreement on a new statement of enhanced privacy principles. We have more than four decades of experience implementing privacy standards for federal agencies, and that is a useful base to build on.

---

[2] Priscilla Regan, Legislating Privacy 77 (1995).

[3] Paula Bruening, Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy (2014), Blogs@Intel, http://blogs.intel.com/blog/rethink-privacy-2-0-and-fair-information-practice-principles-a-common-language-for-privacy/.

[4] See Robert Gellman, FAIR INFORMATION PRACTICES: A Basic History (2021 and occasionally updated) at 44, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[5] See, e.g., Markkula Center for Applied Ethics, The Ethics of Online Privacy Protection (2013), https://www.scu.edu/ethics/privacy/the-ethics-of-online-privacy-protection/.

A law focused solely on the federal government makes the task somewhat easier than a similar undertaking that affects other record keepers, especially those in the private sector. Even so, the diversity of the federal government's agencies and activities calls for finding the right balance between privacy, cost, administrative burden, and responsibility. This remains a significant challenge and a more difficult task than in the past because of the relentless changes in technology and a more knowledgeable and demanding public.

The goal here is to propose a replacement for the Privacy Act of 1974 rather than to change that Act piecemeal. That was a fundamental choice I made at the beginning of this project. The Act's assumptions about technology and administration are so far removed from the reality of today that fixing the law's numerous problems through minor adjustments is unlikely to succeed. Nevertheless, some of the broad approaches and specific provisions in current law remain relevant and useful. Some language can be ported, with minimal or no change, to a new law. We are, to some extent, prisoners of what was done in the past. Evolutionary rather than radical change is likely to succeed with less effort and more acceptance. We also have a body of settled case law interpreting existing legislative language, and there is good reason to leave much of that alone. New words for their own sake would require years of litigation to clarify.

The overarching goal of the Privacy Act Project is to redraft the Privacy Act of 1974 and to provide an explanatory report.

The broad objectives of the redraft are:

1. Bring the Privacy Act of 1974 up to date in recognition of current approaches to privacy protection, modern personally identifiable information processing activities, and new information technologies.

2. Preserve the individual rights in existing law and make it easier for individuals to exercise those rights.

3. Allow agencies to implement their responsibilities in a more efficient and more effective way.

4. Make the new Act consistent with other relevant information management laws, while bringing most privacy-related obligations under one legislative framework.

In keeping with modern practice, the redrafted law seeks to be as technologically neutral as possible. A goal of absolute technological neutrality may be impossible to meet. Any law is likely to require revision at some time in the future no matter how technologically neutral it tries to be.

There was sentiment from some project participants to take a bigger bite of information management and information policy law beyond the Privacy Act. They wanted to revise and reenact additional laws under a single consistent and coherent framework. Other information laws for federal agencies address records management, records disposal and archiving, public information collection, data inventories, information security, information quality, evidence-based policy, freedom of information, and more. I agree that this broader task is worth doing. I agree that our information management and information policy laws (and institutions) suffer from a lack of coordination.

However, the broader task would be much harder to do, take an additional year or two, and require more assistance from even more knowledgeable individuals. My assessment is that revising the Privacy Act of 1974 is doable and passable under the right circumstances. Taking on these other related matters, some more visible and more political, might produce a bill so broad and cumbersome as to be unpassable. A bigger revision would also tread on the jurisdictions of multiple congressional committees, and legislation of interest to more than one committee is much harder to pass. I fear that the broader task is simply undoable as a practical matter. Like it or not, we may be doomed to revision of these laws one by one.

A note on terminology. The Privacy Act of 1974 is Public Law 93-579, Act of December 31, 1974, 88 Stat. 1896. Section 3 of the Act amended title 5 of United States Code by adding a new section. That section, 5 U.S.C. § 552a, is what most people mean when they refer to the Privacy Act of 1974. In this report, the Privacy Act of 1974 (or just Privacy Act) refers to that section of United States Code. I discuss other sections of the original public law occur occasionally in this report and explain them in context. Most, but not all, of the other sections from the original public law are obsolete.

Part II. Background and History

A. Background

Laws, like technologies, become outdated. This is the case with the Privacy Act of 1974.[6] The Act originated with concerns about increasing computerization of personal information in the 1970s. In 1972, Elliot Richardson, Secretary of the Department of Health, Education and Welfare, established the Advisory Committee on Automated Personal Data Systems (HEW Advisory Committee). The Committee's charge included analyzing the privacy and other risks posed by automated data systems containing information about individuals maintained by both public and private sector organizations.

The HEW Advisory Committee's seminal 1973 report, *Records, Computers and the Rights of Citizens*,[7] had two main consequences. First, the committee proposed a code of Fair Information Practices (FIPs) for automated personal data systems.[8] FIPs took over the privacy policy world during the next decade.[9] Even today, almost 50 years later, FIPs are internationally recognized practices for addressing the privacy of information about individuals.[10] FIPs provide the underlying policy for many national laws addressing privacy and data protection matters.[11] The international policy convergence around FIPs as

---

[6] Public Law 93-579, 88 Stat. 1896, Act of Dec. 31, 1974. Section 3 of the Public Law, the main section of the Act, codified at 5 U.S.C. § 552a, is the part of the Act most commonly referred to as the Privacy Act of 1974. The other sections of the Public Law contained findings and purposes (§ 2), a restriction on the collection of Social Security Numbers by federal, state, and local government agencies (§ 7), or are obsolete.

[7] Available at the Electronic Privacy Information Center's website, http://epic.org/privacy/hew1973report/default.html. For transcripts of the meetings of the Committee, see Archive of the Advisory Committee on Automated Personal Data Systems, Berkeley Law, University of California, https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/.

[8] See generally Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, 12 IEEE Security & Privacy 51 (2014), https://www.computer.org/csdl/magazine/sp/2014/04/msp2014040051/13rRUwInvHy. See also Deirdre K. Mulligan, *The Enduring Importance of Transparency*, 12 IEEE Security & Privacy 61(2014), https://www.computer.org/csdl/magazine/sp/2014/03/msp2014030061/13rRUx0xPGT; K Evans, *Where in the World Is My Information?: Giving People Access to Their Data*, 12 IEEE Security & Privacy 78 (2014), https://ieeexplore.ieee.org/abstract/document/6924623/.

[9] For a history of FIPs, see Robert Gellman, FAIR INFORMATION PRACTICES: A Basic History (2021 and occasionally updated), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf. This history sets out the full text of the original version of FIPs from the HEW Committee, as well as subsequent versions from other sources.

[10] Others contributed in major ways to the development and adoption of FIPs, most notably the Organisation for Economic Cooperation, Development, the Council of Europe, and the United Kingdom's 1972 Committee on Privacy chaired by the Rt. Hon. Kenneth Younger. See id.

[11] See Graham Greenleaf and Bertil Cottier, 2020 Ends a Decade of 62 New Data Privacy Laws, 163 Privacy Laws & Business International Report 24-26 (2020) ("The decade 2010-2019 has seen 62 new countries enacting data privacy laws, more than in any previous decade, giving a total of 142 countries with such laws by the end of 2019"), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.

core elements for information privacy has remained in place since the late 1970s.[12] Today, FIPs tend to be viewed as necessary but no longer sufficient for a complete privacy policy.

Second, the HEW Committee also recommended that Congress enact protections for administrative personal data systems. Privacy had been a topic of congressional interest for a decade, and the HEW Committee's recommendations came at an opportune moment. Following the Committee's report, the Privacy Act of 1974, based largely on the Committee's recommendations, became law just before the end of the 93rd Congress in 1974.[13] Some called the law a Watergate reform, but the Privacy Act had deep roots in congressional activities that predated Watergate by a decade or more.

The Privacy Act of 1974 reflected the information technologies in current use in the 1970s. One "technology" was the file cabinet, a commonly used means of storing information on paper. However, it was the increasing use of computers and their growing sophistication that most captured public and congressional attention and concern. The HEW Committee noted the need to "establish standards of record-keeping practice appropriate to the computer age."[14] Looking back, we see the 1970s as the dawn of the era of the mainframe computer. A typical mainframe computer was large, typically filling one or more air-conditioned rooms. Using the computer required a centralized staff with specialized knowledge and skills to operate and program mainframe computers. The findings in the original law reflected concern about the consequences of computers:

> The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.[15]

There is no need here to make a lengthy case about how much information technology has changed since 1973. Modern computers are smaller, immensely powerful compared to their predecessors, maintain vast amounts of information, controllable by average users, and they can share information broadly via the Internet and in other ways.[16] Many of the practical considerations that served to

---

[12] Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States at 991992). Bennett's book discusses how international privacy policy converged about FIPs during the 1970s and 1980s. http://www.cornellpress.cornell.edu/book/?GCOI=80140100026690.

[13] Public Law 93-579, 88 Stat. 1896 (1974).

[14] HEW Report at xx.

[15] Public Law 93-579, § 2(a)(2), 88 Stat. 1896 (1974).

A few years later, the Commission on Federal Paperwork raised some of these same issues in a different context. The Paperwork Commission also raised awareness about on the need to better manage information resources, including resources related to privacy. Information resources management (IRM) is now a focus of attention by the management part of the Office of Management and Budget, and OMB includes its privacy activities as part of IRM. See, e.g., Commission on Federal Paperwork, Final Summary Report (1977), https://www.google.com/books/edition/_/g1tQfCFXiZoC?hl=en; Office of Management and Budget, Circular A-130, Managing Information as a Strategic Resource (2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf. Appendix II of Circular A-130 addresses responsibilities for managing personally identifiable information.

[16] See, e.g., Tibi Puiu, Your smartphone is millions of times more powerful than all of NASA's combined computing in 1969, ZME Science (Feb. 15, 2019), https://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/.

protect privacy in the past – including cost, capacity, stovepipe systems, paper files, and technical expertise – no longer function in the same way.[17] The consequences of technology (current and future) on privacy continue to expand, although not necessarily at the same pace as the technology. Still, even though those consequences are greater and even though the public is both more knowledgeable and more concerned, adoption of new technology continues apace. There is no reason to think that this will change.

B. Selected History

1. Privacy Protection Study Commission Assessment of the Privacy Act (1977)

Section 5 of Public Law 93-579 established the Privacy Protection Study Commission (PPSC) as a temporary study commission.[18] The PPSC was a compromise between a Senate bill that proposed an independent Privacy Protection Commission covering all personal record keepers and a House bill that did not include a privacy agency. The need for a privacy agency in the United States remains an issue today, decades later, even after much of the rest of the world enacted privacy and data protection laws that provide for an independent privacy authority.

The Commission operated from 1975-77, publishing its final report in 1977.[19] Appendix 4 to the main Commission report focused on the Privacy Act of 1974.[20] This work represented the first significant review of the Act and its implementation. There have been no other comprehensive reviews of the Act in the intervening years.

The PPSC's assessment is lengthy and cannot be summarized easily. It includes many detailed observations, and the details matter. The preface to the report offers a still-relevant comment on the tradeoff between flexibility of implementation and complying with the goals of the law. The Commission found that agencies took advantage of flexibility in unwelcome ways.

> In many instances, the difficulty with the current law does not appear to arise from the flexibility of implementation it allows, but rather from the fact that agencies have taken advantage of that flexibility to contravene its spirit. Yet, making the law less flexible is not a desirable solution. Implementation costs would rise dramatically, and new developments in information technology could invite uncontrollable circumvention of rigidities in the statute. Hence, our approach has been to strengthen implementation flexibility while striving for clarity of interpretation and providing

---

[17] See generally, Tekla S. Perry, Arm CEO on 5G, The 5th Wave of Computing, and the trillion device world, IEEE Spectrum (Oct. 17, 2018), https://spectrum.ieee.org/view-from-the-valley/computing/embedded-systems/arm-ceo-on-the-5th-wave-of-computing-5g-and-the-trilliondevice-world.

[18] Public Law 93-579, 88 Stat. 1896, Act of Dec. 31, 1974.

[19] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977), https://aspe.hhs.gov/report/personal-privacy-information-society.

[20] Privacy Protection Study Commission, *The Privacy Act of 1974: An Assessment* (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

> incentives for agencies to comply. This preserves the autonomy of each agency to decide how best to comply with each requirement.[21]

The PPSC offered three broad conclusions about the Act:

- The Act represents a large step forward but has not resulted in the general benefits to the public that "either its legislative history or the prevailing opinion" would lead one to expect.
- Agency compliance is difficult to assess because of the ambiguity of some provisions. On the whole, the Commission found agency compliance to be neither deplorable nor exemplary.
- The Act ignores or marginally addresses some data policy issues of major importance.[22]

The PPSC suggested three more specific conclusions as directions to the Congress to fixing the problems;

- The ambiguous language in the Act should be clarified to minimize variations in interpretation but not implementation.
- Any clarification should incorporate *reasonableness tests* to allow flexibility to take into account diverse agency record keeping requirements and future technological developments.
- Reliance on *systems of records* as the trigger for activating the Act's requirements should be abandoned for an approach that activates specific requirements as warranted.[23]

The report elaborated on the significance of the third point regarding the Act's reliance on system of records as:

> … central to the operation of the Act. From an examination of both the language of the Act and its legislative history, it seems clear that the intent of Congress was to include in the definition of the term "record" every one that contains *any* kind of individually identifiable information about an individual. However, because the Congress was mindful of the burden such a definition could impose on an agency, it limited the Act's coverage to records retrieved from a "system of records" by "name . . . or identifying number, symbol, or other identifying particular . . .." *[5 U.S.C. 552a(a)(5)]* Thus, unless an agency, in fact, retrieves recorded information by reference to a "name . . . identifying symbol, or other identifying particular . . .," the system in which the information is maintained is not covered by the Act. Whereas the current record definition refers to information about an individual which *contains* his name or identifier, the system-of-records definition refers to information about an individual which is *retrieved* by name, identifier, or identifying particular. As indicated in Chapter 1 above, the crucial difference is obvious, and the effect has been wholesale exclusion from the Act's scope of records that are not accessed by name, identifier, or assigned particular. None of the Act's protections accrue to an individual whose record is so treated.

---

[21] Id. at Preface.

[22] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) at 502-03.

[23] Id. at 503.

> There are many examples of readily accessible individually identifiable agency records that are not retrieved by personal identifier, and current and emerging computer and telecommunications technology will create more. While the language of the Act speaks in terms of retrieval by discrete individual identifiers, most automated record systems facilitate identification of an individual's record based on some combination of the individual's attributes or characteristics, natural or assigned, as well as by reference to individual identifiers in the more conventional sense. Thus, it would be easy to program a computer to locate particular individuals through attribute searches (e.g., "list all blonde, female Executive Directors of Federal Commissions"). Retrieval of individually identifiable information by scanning (or searching) large volumes of computer records is not only possible but an ever-increasing agency practice. The Federal Trade Commission, for example, is transcribing all written material in its litigation files for computer retrieval, thereby making it possible to search for all occurrences of a particular name, or any other character pattern for that matter.
>
> In summary, the system-of-records definition has two limitations. First, it undermines the Act's objective of allowing an individual to have access to the records an agency maintains about him, and second, by serving as the activating, or "on/off switch" for the Act's other provisions, it unnecessarily limits the Act's scope. To solve this problem without placing an unreasonable burden on the agencies, the Commission *believes the Act's definition of a system of records should be abandoned and its definition of a record amended*.[24]

For present purposes, I took it as especially noteworthy that the earliest review of the Privacy Act of 1974 concluded that the system of records concept was a failure and undermined the Act's objective. The PPSC also made numerous other recommendations for changes to the Act, including a recommendation for the creation of an independent privacy agency.[25] However, Congress gave no serious consideration to the recommendations of the PPSC for amending the Privacy Act of 1974, and the PPSC report faded into the background as is often the case with reports of temporary study commissions. By contrast, the HEW Committee's report was a significant exception to the transitory importance of study commissions, as its contribution of FIPs to international privacy policy remains front and center today. The PPSC report is rarely discussed today.

2. House Government Operations Committee (1983)

Who Cares About Privacy?: Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress (H. Rept. 98-455, 98th Cong., 1st Sess. 1983).[26]

---

[24] Privacy Protection Study Commission, *The Privacy Act of 1974: An Assessment* (1977) (Appendix 4) at 78-79 (footnotes omitted).

[25] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) at 37. For a history of early proposals to establish a U.S. privacy agency, see Robert Gellman, A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board, 54 Hastings Law Journal 1183 (2003), https://repository.uchastings.edu/hastings_law_journal/vol54/iss4/8/.

[26] In the interests of full disclosure, I was the subcommittee staff member who organized the hearings and who wrote the committee report discussed here.

In the 98th Congress, the Committee on Government Operations of the House of Representatives was mostly an oversight committee, but it had legislative jurisdiction over the Privacy Act of 1974. Oversight of the Privacy Act by the Committee over the years ranged from fitful to non-existent. In 1983, however, the Committee (acting through its Subcommittee on Government Information, Justice, and Agriculture) conducted a hearing on the Act and produced an oversight report. At the first day of the hearing, Subcommittee Chairman Glenn English observed that no oversight hearings on the Act had been held since its enactment.[27] At the hearings and in the report, one of the major topics was the role of the Office of Management and Budget (OMB). The original Public Law assigned OMB responsibility to (1) develop guidelines and regulations for the use of agencies in implementing the Act, and (2) provide continuing assistance to and oversight of the Act's implementation by the agencies.[28]

The Committee report's findings centered on the role of OMB, concluding that interest in the Privacy Act by OMB "has diminished steadily since 1975."[29] The Committee recommended that OMB should be more aggressive in raising Privacy Act issues and in monitoring agency compliance with the OMB guidelines on the Act.[30]

The report raised several other issues that later became important.[31] First, the report discussed the growing use of computer matching.

Second, the report found that privacy interests frequently conflict with other important governmental interests such as economy and efficiency. The report found that "there is a constant risk that privacy concerns will not be fully or fairly considered by federal agencies." In later legislation, Congress added a requirement that agencies prepare Privacy Impact Assessments before developing or procuring

---

[27] Oversight of the Privacy Act of 1974, Hearings before a Subcommittee of the House Committee on Government Operations, 98th Congress, 1st Session (1983), https://babel.hathitrust.org/cgi/pt?id=uc1.31210012875835;view=1up;seq=2.

[28] Public Law 93-579, § 6, Act of Dec. 31, 1974, 88 Stat. 1896, 1906. As part of the Computer Matching and Privacy Protection Act Amendments of 1989, Public Law 100-503, Congress moved the language from the 1974 Public Law about the role of OMB to subsection (v) of 5 U.S.C. § 552a. The only substantive change was the addition of language directing OMB to prescribe guidelines and regulations *after notice and opportunity for public comment*. The Computer Matching Amendments also assigned OMB various roles in oversight of agency computer matching activities.

[29] *Who Cares About Privacy?: Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, Report of the House Committee on Government Operations, House Report 98-455 at 35 (1983).

[30] Id. at 2. Committee Member John Erlenborn filed separate views stating that a limited role for OMB was contemplated at the time of the Act's passage and that Congress intended the agencies to handle implementation without central direction beyond the initial implementation period. Erlenborn was one of the Republican floor managers at the time of the Act's passage. Id at 56 (Separate Views of Hon. John N. Erlenborn). Other Republican Members of the Committee agreed with the report's recommendation for more oversight by OMB. Id. at 58 (Separate Views of Hon. Thomas N. Kindness, Hon. Frank Burton, Hon Lyle Williams, Hon. Dan Burton, Hon. Tom Lewis, Hon. Alfred A. (Al) McCandless, Hon. Larry E. Craig, and Hon. Dan Schaffer).

[31] See id. at 36-37.

information technology that collects, maintains, or disseminates identifiable information or before initiating new collections of personally identifiable information.[32]

Third, the report notes that the Privacy Act of 1974 only gave rights to U.S. citizens and resident aliens. At the time, the Reagan Administration proposed restricting the ability of foreign nationals to use the Freedom of Information Act, which provides a method of access to personal records for those denied use of the Privacy Act of 1974. The report recommended that the Reagan Administration "reconsider" its proposal to deny foreign nationals the ability to use the FOIA. The FOIA restriction never became law, but the limits of the Privacy Act became an issue later.

Fourth, the report also discussed the possible need for a privacy agency, suggesting that Congress should consider alternatives to OMB as a privacy oversight agency.

A second part of the Committee report summarized Privacy Act oversight activities of the Committee. The Privacy Act requires agencies to submit proposals for new systems of records and for new routine uses to the Congress. The report summarized subcommittee responses to these proposals during the period from 1977 through 1982.

3. GAO Reports (1977-2014)

The Government Accountability Office (formerly General Accounting Office) reviewed aspects of Privacy Act of 1974 implementation at various times over the years.[33] It is difficult to generalize from GAO's findings from so many reports. Some themes are 1) a variance of compliance efforts by agencies; 2) unclear or inadequate guidance; 3) technological changes presenting new risks; 4) varied

---

[32] E-Government Act of 2002, Pub. L. 107–347, § 208, Act of Dec. 17, 2002, 116 Stat. 2910, 44 U.S. § 3501 note. The discussion of PIAs in the section-by-section part of this report states that the requirement in this Act was so limited that it often fails to contribute usefully to the evaluation of privacy consequences.

[33] See, e.g., Government Accountability Office, FBI Taking Actions to Comply Fully with the Privacy Act (1977) (GGD-77-93), https://www.gao.gov/products/GGD-77-93; Government Accountability Office, Agencies' Implementation of and Compliance with the Privacy Act Can Be Improved (1978) (LCD-78-115), https://www.gao.gov/products/LCD-78-115; Government Accountability Office, Privacy Act of 1974 Has Little Impact on Federal Contractors (1978) (LCD-78-124), https://www.gao.gov/products/LCD-78-124; Government Accountability Office, Privacy Act: Federal Agencies' Implementation Can Be Improved (1986) (GGD-86-107), https://www.gao.gov/products/GGD-86-107; Government Accountability Office, Privacy Act: Privacy Act System Notices (1987) (GGD-88-15BR), https://www.gao.gov/products/GGD-88-15BR; Government Accountability Office, Peer Review: Compliance with the Privacy Act and Federal Advisory Committee Act (1991) (GGD-91-48), https://www.gao.gov/products/GGD-91-48; Government Accountability Office, Privacy Act: OMB Leadership Needed to Improve Agency Compliance (2003) (GAO-03-304), https://www.gao.gov/products/GAO-03-304; Government Accountability Office, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information (2008) (GAO-08-536), https://www.gao.gov/products/GAO-08-536; Government Accountability Office, Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions (2008) (GAO-08-603), https://www.gao.gov/products/GAO-08-603; Government Accountability Office, Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape (2012) (GAO-12-961T), https://www.gao.gov/products/GAO-12-961T; Government Accountability Office, Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation (2014) (GAO-14-44), https://www.gao.gov/products/GAO-14-44.

supervision; and 5) shortcomings with the Act itself. Nothing in the GAO reports attempts to compare compliance with the Privacy Act of 1974 with the level of compliance of other laws imposing administrative requirements. It is well-known that compliance with the Freedom of Information Act[34] – a law sometimes implemented by the same agency offices responsible for the Privacy Act of 1974 – has been highly variable over the years.[35]

The incomplete picture suggested by these reports nevertheless supports the core conclusion here, namely that the Act is out-of-date and needs revision. A revised law can better protect the privacy interests of data subjects and reduce some of the implementation problems and uncertainties that characterize the existing law.

[34] 5 U.S.C. § 552.

[35] The GAO website identifies numerous reports on FOIA compliance, and the level of user complaint and litigation with the FOIA have been higher than with the Privacy Act of 1974. Some of the differences are a consequence of greater usage of the FOIA by the public and the often greater "stakes" involved in FOIA matters. Further, nothing in the Privacy Act provides judicial oversight of agency implementation comparable to the voluminous litigation that the FOIA engendered. The proposed bill includes a process to increase the possibility of judicial review of agency privacy activities by public interest groups and others.

Part III. Major Issues

A. Privacy Act Systems of Records

1. Existing Law

The key organizing concept for the Privacy Act of 1974 is the *system of records*. A *record* is:

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[36]

This is an expansive definition ("including but not limited to") that encompasses virtually every type of information associated with an individual.

A *system of records* is:

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[37]

The most noteworthy feature of a system of records is that information must be retrieved (not just retrievable) by individual identifier. Thus, the test for whether a collection of records is a system turns on whether the agency in fact retrieves records by individual identifier. It is a question of fact. Consider two files containing correspondence. One file organizes the letters by the name of the recipient. That file is likely to be a system of records because records are filed and, more importantly, retrieved by name. The other file organizes the letters by date. That file is not likely to be a system of records because the records would be retrieved by date rather than an individual identifier. By varying how or if records are retrieved from these files, either could be a system of records or not. It is not clear from the definition whether a single retrieval of a single record by name makes a collection of records a *system of records* or if retrieval must be a regular activity. In most cases, it will not matter.

The Privacy Protection Study Commission report observes that the definition comes from a manual model of information processing rather than a computer-based model.[38] In suggesting revisions to the Privacy Act, the PPSC introduced some new concepts, but its suggested revision of the definition of *system* still relied on the notion of an *established retrieval scheme or indexing structure*.[39] The PPSC recognized the potential ease of record retrieval from a computer file, but it still stuck to the idea of

---

[36] 5 U.S.C. § 552a(a)(4).

[37] Id. at (a)(5).

[38] Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 6 (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

[39] Id. at 119.

retrieval as part of the definition. Computers of the mid-1970s did not allow for easy or on-demand retrieval.

The system of records concept was important to the public notice element of the Act. The Act requires each agency to publish in the Federal Register a notice of the existence and character of each system of records that it maintains.[40] A system of records notice or SORN – the acronym is commonly used to refer to either the notice or to the system of records itself – is extensive and must include these elements:

> (A) the name and location of the system;
> (B) the categories of individuals on whom records are maintained in the system;
> (C) the categories of records maintained in the system;
> (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
> (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
> (F) the title and business address of the agency official who is responsible for the system of records;
> (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
> (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
> (I) the categories of sources of records in the system.[41]

The publication requirement fulfilled what the PPSC called a "prime objective" of the Act, which was to ensure that there are no secret agency record keeping systems.[42] While many systems of records can be exempted from various requirements of the Privacy Act, no system is exempt from the requirement to publish a description. The USA FIPS Act continues the policy of no secret agency record keeping activities.

Many agency SORNs today are out-of-date, incomplete in some ways, or wrong in material and immaterial ways. Nevertheless, the requirement that agencies publish system notices was in some ways a significant success of the Privacy Act. Prior to 1975, many agencies had no idea what records they maintained. The public had even less knowledge about agency record keeping activities before the publication of Privacy Act notices.

In some cases, it took agencies a long time (and years beyond the original deadline) to find and describe all their systems of records. Preparation for the initial publication of system notices resulted

---

[40] 5 U.S.C. § 552a(e)(4).

[41] Id.

[42] Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 10 (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

in the elimination of many duplicative or unnecessary data systems.[43] The Act forced agencies to do a better job of managing their personal records systems. That the agencies did not carry out the publication requirement well at the beginning and that there are still shortcomings in agency publications does not mean that publication of system notices is not worth doing. The publication of Privacy Act system notices provides a wealth of information to the public (and to the agencies themselves) that was largely unavailable before the Act.[44] Notwithstanding all of the implementation shortcomings, publication of notices was one of the Act's successes.

Given the simplicity of indexing and retrieving information on a modern computer system, defining a system of records using any type of retrievability test is pointless. Even an untrained computer user can retrieve unstructured data on a computer virtually at will. Under the current definition, any act of retrieval could, in theory, create a new system of records. This possibility has been long ignored by the government's privacy establishment, but everyone is stuck with the definition in current law.

Agencies interpret the concept of a system of records in variable ways. For example, some agencies treat electronic mail systems as systems of records because email is indexed and retrieved by the name of the sender/recipient. Other agencies deem electronic mail to be a work-related activity that is not "about an individual" so they do not have systems of records notices for email systems. This diversity of interpretation should not exist.

Other noteworthy words in the definition of *system of records* are: "any item, collection, or grouping of information about an individual **that is maintained by an agency**." When an agency uses records maintained by third parties as part of an agency function, those external records are not part of the agency's systems of records. An example of a third-party record used by an agency is a credit record maintained and owned by a consumer reporting agency.[45] If an agency consults an external database and copies information into its system of records, that information becomes subject to the Privacy Act and may be accessible to the data subject. Otherwise, however, that external data may not be covered by or even discussed in a system of records notice.

2. Other Suggested Approaches to Systems of Records

a. Privacy Protection Study Commission

In its 1977 report, the Privacy Protection Study Commission proposed a revision of the Privacy Act. Its suggested definition of *system* or *subsystem* was:

> any collection or grouping of individually identifiable records which is systematically filed, stored, or otherwise maintained according to some established retrieval scheme

[43] See Robert Gellman, Does Privacy Law Work? at 196 in Philip E. Agre & Marc Rotenberg, Technology and Privacy: The New Landscape (1997).

[44] See, for example, Privacy Act Issuances, a resource maintained on a website by the Office of the Federal Register. The website lists all system of records notices for all agencies dating back to 1995. https://www.govinfo.gov/app/collection/PAI/. Originally, the Federal Register offered a compilation of all agency systems of records in five printed volumes.

[45] Consumer Reporting Agencies generally provide consumer reports and risks scores to a variety of businesses. See *List of Consumer Reporting Agencies,* Consumer Financial Protection Bureau (2020), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list.pdf.

> or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the record, or any portion thereof, on the basis of the identity of, or so as to identify, an individual or individuals.[46]

The Commission also proposed a new term, *accessible record* to mean:

> an individually identifiable record, except a research or statistical record, which is:
> (A) systematically filed, stored, or otherwise maintained according to some established retrieval scheme or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the record, or any portion thereof, on the basis of the identity of, or so as to identify, an individual, or
> (B) otherwise readily accessible because:
> (i) the agency is able to access the record without an unreasonable expenditure of time, money, effort, or other resources, or
> (ii) the individual to whom the record pertains is able to provide sufficiently specific locating information so as to render the record accessible by the agency without an unreasonable expenditure of time, money, effort, or other resources.[47]

These terms seem rooted in the computer technology of the day that typically required programming to index and retrieve records. The terms do not seem useful today.

b. Akaka Bill

In the 111th and 112th Congress, Senator Daniel Akaka started what may have been the only serious congressional effort to revise the Privacy Act of 1974. His bill amending the Act saw no formal action during the 112th Congress (2011). Its definition for system of records was:

> a group of any records maintained by, or otherwise under the control of any agency that is used for any authorized purpose by or on behalf of the agency.[48]

This approach was more attuned to a world of computerized records because it drops all references to the notion of retrievability. Instead, the focus is on groups of records, a more technologically neutral concept. The definition includes records maintained by an agency and adds the notion of records *under the control* of an agency. That may be a reference to contractor records, but it would not cover wholly third-party records that an agency does not control.

c. European General Data Protection Directive

The European General Data Protection Directive, a 2016 law, takes a different approach. Article 2 of the GDPR defines the scope of the regulation:

---

[46] Id. at 154.

[47] Id.

[48] S.1732, 112th Cong., 1st Sess. § 2(a)(2) (2011), https://www.congress.gov/bill/112th-congress/senate-bill/1732.

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[49]

A filing system is "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."[50] While it is clear that the regulation seeks to be technologically neutral, there is little in the regulation that explains either *filing system* or *specific criteria or structured set*. These three concepts imply retrievability and perhaps linkability as essential elements. The GDPR used the same language and concepts as the EU Data Protection Directive that the GDPR replaced.[51] Given the GDPR's applicability to a broad set of personal data controllers (i.e., virtually every data controller in the private, and non-profit sectors and most in the public sector), retaining a focus on retrievability may still make some sense.

An important difference between the EU approach and the Privacy Act of 1974 is that the notion of *filing system* in EU rules does not appear to be an important concept to privacy regulation in the same way that *system of records* is central to the Privacy Act. In both the Data Protection Directive and the GDPR, filing systems are discussed in the recitals[52] and defined. But there is little about filing systems in the operative parts of the documents. It may be a remnant related to the increasingly insignificant distinction between paper and computer records.

Importantly, there is no general requirement in the GDPR to notify the public about filing systems maintained by a data controller. There was and continues to be an obligation to provide information about processing to the data subject.[53] However, general public notice of processing activities is not required.

---

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, art. 2, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[50] Id. at art. 4(6).

[51] Council Directive 95/46, art. 2(c), Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[52] Recital 15 provides: "In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation." GDPR at Recital 15. The UK Information Commission's Office has a 2011 explanation that suggest the notion of a filing system makes the same distinction between a file indexed by name and a file indexed by date that the Privacy Act of 1974 makes. Information Commissioner's Office (UK), Frequently asked questions and answers about relevant filing systems (May 2011), https://ico.org.uk/media/for-organisations/documents/1592/relevant_filing_systems_faqs.pdf.

[53] GDPR at Article 13 (Information to be provided where personal data are collected from the data subject) and Article 14 (Information to be provided where personal data have not been obtained from the data subject). EU Data Protection Directive at Article 10 (Information in cases of collection of data from the data subject) and Article 11 (Information where the data have not been obtained from the data subject).

The earlier 1995 Data Protection Directive originally provided for a register of "processing operations." This could have been a rough equivalent of the publication of system of records notices. The Data Protection Directive included a requirement for data controllers to notify their supervisory authority "before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."[54] The Directive also specified the content of the notification, which bears rough similarity to the content of a Privacy Act system of records notice.

> 1. Member States shall specify the information to be given in the notification. It shall include at least:
> (a) the name and address of the controller and of his representative, if any;
> (b) the purpose or purposes of the processing;
> (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
> (d) the recipients or categories of recipient to whom the data might be disclosed;
> (e) proposed transfers of data to third countries;
> (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.[55]

The Directive gave Member States authority to establish broader notification requirements or to allow for exemptions. The Directive also required Member States to provide a public register of processing operations.[56]

However, in practice, notification turned out to be difficult, expensive, and not useful for monitoring. As the Article 29 Working Party wrote in a document on notification in 1997 (almost a year prior to the effective date of the Directive):

> Some of these countries are currently simplifying the notification requirements or introducing exemptions from the obligation to notify. The general systems of notification have in some cases proven to be very resource consuming for the data protection authorities. Furthermore it turned out to be difficult to perform any substantive monitoring on the basis of notifications.[57]

A 2002 comparative summary of national laws found widespread noncompliance with notification under earlier national data protection laws and little improvement under the Directive.

> There is no evidence that this situation has significantly improved in the above-mentioned countries, or is any different in the other Member States: the percentage of registered controllers compared to the number of companies in a country (in my opinion, the best first indication of the level of compliance with notification) remains

---

[54] EU Data Protection Directive at Article 18(1).

[55] Id. at Art. 19

[56] Id. at Article 21(2).

[57] Article 29 Working Party, Working Document: Notification at 4 (1997) (WP 8), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp8_en.pdf.

> everywhere very low indeed. One reason why notification is not more strongly pursued is that the data protection authorities in fact largely agree that the notified particulars are a very poor indication of what goes on in practice (even if they faithfully reflect what goes on, which is doubtful in itself, as discussed in the next section); and that it adds little if anything to compliance with the more onerous requirements of the laws. According to the UK data protection authority, the system may even have a negative effect on compliance, in that it suggests that controllers who have notified their operations act in accordance with the law, although in practice there is no certainty that this is the case at all.
>
> Many of the authorities would therefore prefer to spend their resources on other measures which could contribute more effectively to compliance by controllers and to the protection of the interests of the data subjects. However, others believe that notification does have an "educational" effect, in that it forces controllers to examine their operations in the light of the law.[58]

Ultimately, the GDPR did not repeat the notification/registration that started with the Directive so there is no EU-wide requirement today. This is not to suggest that there is no accountability for data controllers, just that there is no mandated public register of filing systems like that required by the Privacy Act of 1974.[59]

3. A Better Approach

A different approach to organizing privacy rules – proposed here for the first time – focuses broadly on agency activities rather than narrowly on record systems. The term used in the proposal is *agency activity affecting privacy* (or A3P), which means:

> agency function, program, or operation that involves the processing of a record about an individual.

The choice of the term here was difficult. Some other options created acronyms that already have established meanings in the privacy realm. The mildly awkward *agency activity affecting privacy* is offset in part by the breezier acronym *A3P*. I decided not to use a superscript (A^3P) because typing a superscript is more cumbersome.

The A3P definition focuses on the purpose of processing rather than on the manner in which an agency files or retrieves personally identifiable information. The idea is that an A3P would provide the

---

[58] Douwe Korff, EC Study on Implementation of Data Protection Directive § 12.1(2002), https://ssrn.com/abstract=1287667. The study also found that the registers by the public was "relatively rare." Id. at § 12.2.

[59] See DLA Piper, Data Protection Laws of the World (2019), https://www.dlapiperdataprotection.com/index.html?c=GB&c2=&t=registration ("In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.").

public with a more understandable view of an agency's personal record keeping by allowing multiple filing systems to be included in the same notice if the systems relate to the same function, program, or operation. The internal details of records organization are of less public interest than the kind of records that an agency processes, the purposes of that processing, and the way in which an agency uses or discloses the records. More details about A3Ps will be found in the section-by-section analysis later in this report.

B. Controlling Disclosures (Routine Uses)

In the Privacy Act, a routine use is a disclosure that is compatible with the purpose for which a record was collected. Defining and controlling disclosures is a major challenge in all privacy laws around the world. I call this challenge the *compatibility problem*. How can we limit disclosures with a statutory standard that offers useful guidance to agencies yet provides the ability to resist pressure for new disclosures that are too remote from the purposes for which records were collected? Frankly, I do not believe that any existing privacy law or policy offers a complete solution to the compatibility problem, and I doubt that there will ever be any word formula alone that will work. The Privacy Act's approach to the compatibility problem is largely a failure.

This section reviews several proposed or current approaches to controlling disclosures. The draft bill proposes a new term, a new definition, and new procedures to address the challenge of authorizing agencies to define disclosures without giving agencies carte blanche to do anything they want.

1. Privacy Protection Study Commission

The Privacy Protection Study Commission (PPSC) summarized problems and concerns that arose during the first few years of the Privacy Act. In its 1977 report, the PPSC noted that some agencies promulgated routine uses that continued disclosures that the agency made prior to passage of the Privacy Act regardless of compatibility.[60] Some routines uses were overbroad, allowing disclosure with few or no restrictions.[61] Some routine uses ignored the procedures for specific disclosures included in the Act itself.[62] Some agencies, at least initially, applied the compatibility test so strictly that previously standard disclosures could not occur and other agencies could not carry out their functions.[63] Many of the problems of restrictive disclosure policies were eventually worked out one way or another.[64] Other

---

[60] Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 62 (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

[61] Id. at 63.

[62] Id. Subsection (b)(7) establishes procedures for disclosure to law enforcement agencies, but agencies established routine uses that evaded those procedures. The problem here was that the statutory procedures were insufficient to meet all law enforcement disclosure needs, but it was never clear under the Act whether agencies could lawfully "evade" those statutory procedures by establishing routine uses to cover the same types of disclosures. Nothing in the Act addressed the issue.

[63] Id.

[64] Id. at 64-5. Solutions resulted because of the pressure from the disruption or potential disruption of operations. However, when an agency established an overly broad routine use, there was no effective source of pressure for restricting the routine use. The practical inability of challenges to agency routine uses informed the new administrative remedy in the proposed bill.

issues that the PPSC observed involved disclosures either required or authorized under other laws.[65] These problems eventually disappeared, often without much regard for the compatibility standard in the Act.

The PPSC proposed to replace the original definition of a routine use with a revised definition and a new concept, the *collateral use*. Under the Commission's proposal, a routine use would be:

> the use or disclosure of an individually identifiable record for a purpose which is:
> (A) compatible with the purpose for which the information in the record was collected or obtained, and
> (B) consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained.[66]

This proposed definition applies to both uses and disclosures. It keeps the original compatibility test but adds a further restriction tied to "reasonable expectations." A problem with this standard is that it compounds the felony. It adds a new and vague concept ("reasonable expectation") to the vague concept ("compatible with the purpose") already in the law. To be fair, it is hard to avoid some degree of vagueness in the end. The difficulty remains writing a policy that provides clear and unambiguous direction for all personally identifiable information processing activities in the federal government.

The PPSC's collateral use would be:

> the use or disclosure of an individually identifiable record for a purpose which:
> (A) would not be considered a routine use as defined by subsection (a)(9) of this section, and
> (B) is specifically authorized by statute, provided, however, that such statute:
> (i) was enacted after January 1, 1975, and
> (ii) establishes specific criteria for the use or disclosure of specific types of information.[67]

Collateral uses would address some of the problems that the PPSC uncovered as well as some of the unresolved legal questions about the scope of authorized disclosures and the relationship between the Privacy Act and other laws. The PPSC explained the goal:

> Because the collateral-use concept presupposes direct, and probably increasing, Congressional involvement in information policy decisions, it should help to keep the relationship between the Privacy Act and other information policy legislation in clear focus. The current law and its legislative history are silent on whether the Act was intended to supersede preexisting statutes authorizing uses or disclosures of information that do not meet the compatible-purpose test. The OMB Guidelines take the position that preexisting statutes which permit less disclosure to third parties than

---

[65] Id. at 65

[66] Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 154 (Appendix B) (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

[67] Id. at 155.

> the Privacy Act allows were not superseded, but there was no basis for concluding that the many sections of the U.S. Code that authorize or require the disclosure of information about individuals to third parties were. Adding the concept of collateral use will assure that in the future the Congress' attention will be drawn to statutorily authorized uses and disclosures that do not meet the compatible-purpose test and also, by virtue of the January 1, 1975 cut-off date, will precipitate a reconsideration of sections of the U.S. Code that do not meet the test today.[68]

One other requirement recommended by the PPSC for both routine uses and collateral uses was certification by the "designated official." The PPSC proposed that each agency head designate an officer to oversee the agency's implementation of the Act.[69] The designated official would have to certify that a routine use or a collateral use met the terms of the statutory definition.[70] Congress ignored the PPSC's recommendations for changing the Privacy Act of 1974.

Rightly or wrongly, routine uses proliferated over time, in part because there was no direct way to challenge a routine use in court other than in a specific case where reliance on a routine use resulted in harm to an individual. In addition, administrative oversight by OMB was inconsistent over the years, and congressional review, inconsistent at best, largely disappeared after the 103rd Congress. Today, some agencies systems of records have large numbers of routine uses. One example, the Department of Veterans Affairs Patient Medical Record System, has 60 routine uses. Three of these are useful for illustration.

> 5. Health care information may be disclosed by appropriate VA personnel to the extent necessary and on a need-to-know basis, consistent with good medical-ethical practices, to family members and/or the person(s) with whom the patient has a meaningful relationship.
>
> 44. VA may disclose information to telephone company operators acting in their capacity to facilitate phone calls for hearing impaired individuals, such as patients, patients' family members, or non-VA providers, using telephone devices for the hearing impaired, including Telecommunications Device for the Deaf (TDD) or Text Telephones.
>
> 48. VA may disclose information to other Federal agencies in order to assist those agencies in preventing, detecting, and responding to possible fraud or abuse by individuals in their operations and programs.[71]

A complete analysis of current routine uses across government would take hundreds of pages or more, but it is easy to critique these three routine uses as examples. The first is largely clear and reasonable.

---

[68] Id. at 120 (footnote omitted).

[69] Id. at 167 (Illustrative revision of the Privacy Act of 1974 at (j).

[70] Id. at 160 (at (d)(4) & (5).

[71] Department of Veterans Affairs, Patient Medical Records-VA (VA 24VA10P2), in Government Printing Office, Privacy Act Issuances (2017), https://www.govinfo.gov/content/pkg/PAI-2017-VA/xml/PAI-2017-VA.xml#24VA10P2.

It is also actually mostly consistent with disclosure standards under the federal HIPAA health privacy rule.[72]

The second quoted routine use serves a legitimate purpose, but it lacks any limit on the scope of information disclosable to telephone company operators. It would be better, for example, if the routine use specifically limited the disclosure to information that the operator needed to facilitate the call. As written, the facilitation language describes the function of the operator rather than limiting the information to be disclosed.

The last of these routine uses is, in my judgment, too ill-defined to satisfy the Act's compatibility test and may well violate HIPAA standards. It is questionable for the breadth of the allowable disclosures, the lack of any apparent relationship between the purpose of collection and the use by *any* federal agency in *any* fraud and abuse program whether related to health care or otherwise, and the absence of an administrative process prior to disclosure or requirement for a determination by VA official of suitable rank prior to a disclosure.

Over time, agencies tended to view the routine use provision as a procedural requirement rather than a substantive limit. The procedure is to publish a notice in the Federal Register. To restate the obligation glibly but consistently with the view of many agencies, any disclosure is permissible as long as the agency publishes the proper notice.

Agencies may overlook in whole or in part the substantive requirement that routine uses be compatible with the purpose for which the record was collected. Agencies also sometimes ignore the public notice purpose of publishing by providing no specificity about what can be disclosed and to whom it can be disclosed. The Central Intelligence Agency offers an example from its list of "general routine uses" applicable to all agency systems of records. The Agency currently has 14 general routine uses, some mundane, and some broadly expansive. The last of these routine uses is:

> 14. In the event that none of the routine uses listed above is applicable, a record from a system of records maintained by the Central Intelligence Agency may be disclosed, as a routine use, to other appropriate recipients, if such dissemination is necessary to a lawful activity of the United States, and the General Counsel of the Central Intelligence Agency, in consultation with the Department of Justice, determines that such dissemination is lawful.[73]

To restate this routine use, it allows the disclosure of anything in any Privacy Act system of records to anyone ("other appropriate recipients") if the disclosure is necessary to a lawful activity of the United States and the Agency's General Counsel determines that the disclosure is lawful. Even for an intelligence agency which admittedly has a need for secrecy in some of its activities, this routine use tells the public nothing about how Privacy Act records might be disclosed. The CIA effectively reserved the right to disclose anything to anybody, although it deserves some credit for requiring a determination by the agency's general counsel. Whether a routine use so broad and so vague meets the existing statutory standard is unclear at best. However, under the Privacy Act, there is no apparent

---

[72] 45 C.F.R. Part 164, https://www.ecfr.gov/cgi-bin/text-idx?SID=54a1c1488d1678d74ff0d46f6ba5b0ce&mc=true&node=pt45.1.164.

[73] https://www.federalregister.gov/documents/2005/07/22/05-13889/privacy-act-of-1974-system-of-records-and-routine-uses.

way for anyone to challenge the breadth of the routine use unless the CIA relied on the routine use, an individual learned of the disclosure, and the individual could prove harm.

2. Computer Matching: A Case Study

Computer matching is the computerized comparison of records from two or more systems of records for the purpose of establishing or verifying eligibility for federal benefit programs. Matching also includes comparisons from a system of records with non-federal agency records.

Matching became a subject of controversy in the late 1970s, when federal agencies sought to use information technology in new ways as part of the routine management of federal benefit programs. The rise of computer matching presented privacy legislation with one of its earliest confrontations with new technological capabilities. Uses of personal data that were impractical prior to computers could now be carried out readily and at little marginal cost.

Computer matching placed pressure on one of the Act's weakest points, the routine use. The battle here pitted privacy against politically popular methods for addressing fraud, waste, and abuse in federal programs. It is worth reviewing the history of the 1988 Computer Matching Amendments at some length because that history is instructive about the problem of controlling disclosures in a general privacy law.

The Privacy Act of 1974 allows agencies to define allowable external disclosures for each system of records. The term that the Act defined for this purpose was *routine use*. In modern privacy practice, a *use* with respect to a record means an activity (e.g., sharing, employment, examination, or transfer) *within* the entity that maintains the record. A disclosure means, with respect to a record, the release, transfer, provision of access to, or divulging in any other manner of the record *outside* the entity holding the information.[74] However, the Privacy Act of 1974 established the term *routine use* to describe external disclosures. That choice of terms was a source of later confusion.

The Act defines a *routine use* to mean, with respect to the disclosure of a record, the use of the record for "a purpose which is compatible with the purpose for which it was collected."[75] The meaning of compatibility has been a thorny issue for implementation of the Privacy Act from the beginning.

---

[74] Subsection (b) of the Act (5 U.S.C. § 552a) establishes the rules governing disclosure of a record from a system of records to any person or another agency. Subsection (b)(1) establishes a policy for disclosures to officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties. That provision governs what is today generally call a *use* of information. 5 U.S.C. § 552a(b)(1). The rest of subsection (b) addresses external disclosures of records. Subsection (b)(3) authorizes agencies to disclose records pursuant to established routine uses.

The distinction between an internal use and an external disclosure can be challenging, especially within large federal cabinet departments that encompass many separate and unrelated functions. Because every agency treats itself as a single agency for Privacy Act purposes, many exchanges of information across programs are internal for Privacy Act purposes.

[75] 5 U.S.C. § 552a(a)(7). The HEW Committee's language for controlling information transfers did not rely on a compatibility test. It suggested that no use be made that is "not within the stated purposes of the system as reasonably understood by the individual" except with informed consent of the individual. HEW Report at 61. Because of the subjective understanding of individuals, it is difficult to translate the HEW Committee's standard directly into legislative language. Congress adopted a compatibility standard instead.

Indeed, what I call the *compatibility problem* plagues nearly all broadly focused privacy laws around the world.

Agencies establish routine uses for each system of records by publishing a Federal Register notice and allowing an opportunity for interested persons to submit "written data, views, or arguments."[76] The process is short of being a full notice-and-comment rulemaking. A system of records may have anywhere from a handful of routine uses to dozens.

The legislative history for the Privacy Act of 1974 discusses the notion of compatibility. The concern was that if the standard for regulating disclosure was too narrow, then essential government activities might be disrupted. If the standard was too broad, then there would be no effective control over disclosures. Because the Act was one of the first general purpose privacy laws anywhere in the world, the uncertainty here is understandable. The original OMB Privacy Act guidelines review the congressional intent with some care and offer further explanation of routine use.

> One of the primary objectives of the Act is to restrict the use of information to the purposes for which it was collected. The term "routine use" was introduced to recognize the practical limitations of restricting use of information to explicit and expressed purposes for which it was collected. It recognizes that there are corollary purposes "compatible with the purpose for which [the information] was collected" that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public.[77]

What is noteworthy here is that OMB found it appropriate to add additional concepts to the idea of compatibility with the purpose of collection. OMB talked about purposes that are appropriate and necessary for the efficient conduct of government and that are in the best interests of both the individual and the public. This hints at one problem with the statutory definition. What if an appropriate activity in the best interest of the public is not related to or compatible with the purpose of data collection? The same question asked in a different way is how broadly should the purpose of data collection be defined? In essence, the question of how broadly to define routine uses became a major issue in computer matching.

In 1977, the Department of Health, Education and Welfare began Project Match, a program to compare computer records of individuals receiving benefits under Aid to Families with Dependent Children with computer records of federal employees.[78] The premise was that anyone on both lists was doing something improper. The Privacy Act question was whether the disclosure of records about federal employees for an activity relating to fraud, abuse, or waste in another program was compatible with the purpose for which the records were collected. There were views on all sides of this question.

---

[76] 5 U.S.C. § 552a(e)(11).

[77] Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28953 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

[78] For an early history of computer matching, see Jake Kirchner, "Privacy-A History of Computer Matching in the Federal Government", Computerworld (Dec. 14, 1981), reprinted in Oversight of the Privacy Act of 1974, Hearings before a Subcommittee of the House Committee on Government Operations, 98th Cong., 1st Sess. at 426 (1983), https://babel.hathitrust.org/cgi/pt?id=uc1.31210012875835.

The general counsel of the Civil Service Commission did not approve of the disclosures on the grounds that information about federal employees was not collected with a view toward detecting welfare abuses.[79] Given the political interest and pressure supporting matching programs, however, OMB intervened and issued guidance about conducting matching programs.[80] The guidance did not really address whether matching programs met the compatibility standard in the law. Instead, it set out procedural requirements for the conduct of matching programs. The guidance seemed to quiet the controversy for a while, and computer matching continued and expanded as if all matching activities met the compatibility standard. Professor Priscilla Regan provided a useful summary of the situation following the 1979 OMB Guidance:

> The purpose of the guidelines was "to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy." However, agencies did not follow the guidelines, the OMB did not monitor agencies' activities, the public and interest groups did not respond to *Federal Register* notices, and there was little congressional reaction. The ideas of integrity and efficiency complemented federal agencies' interests in matching records. But the idea of privacy did not complement the interests of any groups with a role in computer matching, except the individuals under investigation, who generally were not aware that their records were being matched. The balance that might have been achievable between the two ideas was offset by the support of interests on one side and the lack of knowledge on the other. In this policy setting, agency use of computer matching increased.[81]

In his book, The Rise of the Computer State, David Burnham reviewed the history of computer matching. He concluded that the words of the 1979 OMB Guidance were "hollow,"[82] citing the Civil Service Commission's reversal of its ban on matching. Burnham's broader conclusion was about "how technology influences the shape of the law and administrative practice of government programs."[83] Matching continued "despite provisions of law that would appear to prohibit it,"[84] because of the difficulty of denying technology.

Computer matching remained mildly controversial, but there was limited congressional response. Opposition to matching was politically unattractive because of the focus on "welfare cheats" from the Reagan Administration and the constant touting of computer matching results (whether justified or

---

[79] See House Committee on Government Operations, Computer Matching and Privacy Protection Act of 1988, House Report 100-802 at 22 & note 112 (1988) (report to accompany H.R. 4699).

[80] Office of Management and Budget, Privacy Act of 1974: Supplemental Guidance for Matching Programs, 44 Federal Register 23138 (April 18, 1979), https://www.govinfo.gov/app/details/FR-1979-04-18.

[81] Priscilla Regan, Legislating Privacy 87 (1995).

[82] David Burnham, Rise of the Computer State 210 (1983).

[83] Id. at 211.

[84] Id.

not by the facts) by agency Inspectors General.[85] In 1982, OMB revised its matching guidance[86] without seeking public comment.[87] The resulting guidance weakened the 1979 requirements, and one observer described the changes as essentially repealing the original lenient safeguards.[88]

Despite the politics of the issue, Senator William Cohen, a Republican from Maine, picked up the matter a few years later in 1986. Cohen deserves much credit for his willingness to step into a controversial subject and look for a suitable response. Together with Senator Carl Levin, he introduced legislation to regulate computer matching.[89] That began a process that resulted in the matching amendments to the Privacy Act of 1974. The initial effort came too late in the Congress for final action, but the Senators persisted in the following Congress.[90] Cohen's success in the Senate provided considerable political cover for House action. Following the Senate, the House eventually took up the issue, and the Computer Matching and Privacy Protection Act of 1988 became law.[91] I was the House staffer responsible for the 1988 amendments. Quiet support for the effort from the Privacy Act staff at OMB helped to shape the amendments and to overcome internal administrative objections.

The computer matching amendments regulate matching activities in three main ways. First, the law requires that agencies conducting matching programs enter into formal matching agreements specifying the terms, justification, and details of the match. The law specifies eleven separate components of an agreement. Matching agreements must be sent to the Congress and made available to the public upon request.[92] Second, the law requires agencies conducting or participating in matching to establish Data Integrity Boards to review and approve matching agreements.[93] Third, the law provides due process procedures for individuals identified in matching activities. Each agency must independently verify information from a match, provide notice to the individual with a statement of findings, and afford an individual an opportunity to contest the findings.[94] The due process requirements resulted because of significant evidence that government agencies used the unverified findings of matching activities to terminate people from assistance programs. In a

---

[85] Computer matching was the subject of an Office of Technology Assessment report requested by several congressional committees. See Office of Technology Assessment, *Electronic Record Systems and Individual Privacy* (1986), https://ota.fas.org/reports/8606.pdf.

[86] Office of Management and Budget, Revised Supplemental Guidance for Conducting Matching Programs, 47 Fed. Reg. 21656 (Mary 19, 1982).

[87] House Committee on Government Operations, *Who Cares About Privacy?: Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress* 12 (H. Rept. 98-455, 98th Cong., 1st Sess. 1983).

[88] Id. at 13 (quoting Robert Ellis Smith, Publisher of the Privacy Journal).

[89] S.2756, 99th Cong., 2d. Sess. (Aug. 14, 1986), https://www.congress.gov/bill/99th-congress/senate-bill/2756.

[90] S.496, 100th Cong., 1st Sess. (Feb. 5, 1987).

[91] Public Law 100-503, Act of October 18, 1988, 102 Stat. 2507 (1988), http://uscode.house.gov/statutes/pl/100/503.pdf.

[92] 5 U.S.C. § 552a(o).

[93] 5 U.S.C. § 552a(u).

[94] 5 U.S.C. § 552a(p).

significant number of cases, the terminations were unjustified.[95] It was that evidence of unfairness that was the engine that drove the legislation through the Congress, essentially without controversy. The legislation achieved the support of the Reagan Administration largely because it was Senator Cohen's bill (Cohen was a Republican) and because of support from OMB Privacy Act staff. Administration support came despite some agency opposition, largely from those who conducted computer matching.

The focus of the amendments was on administrative procedures and due process more than on the privacy consequences or legality of matching. It is difficult to assess the overall success of the matching amendments, but there are suggestions that the due process procedures worked reasonably well. Many problems that resulted from inaccurate records and from the use of outdated files slowly were resolved. The administrative controls are more of a mixed bag, with some agencies going through the required process mechanically but no real enthusiasm. Agencies and OMB consistently ignored the statutory requirement for showing that matching meet a cost-benefit test.

One reason the legislation was not especially controversial is that the original OMB guidance from 1979 included some features that the legislation adopted. OMB told agencies to prepare matching reports and publish notices in the Federal Register. It did not matter that agencies did not follow the guidance, something that Professor Regan suggested was the case. OMB was hard pressed to oppose ideas it promoted earlier. The due process requirements in the legislation went beyond OMB guidance, but both Senate and House justified the requirements by documenting a record of problems with the use of "raw hits" to deprive individuals of benefits to which they were legitimately entitled.[96] The discrepancies were often the result of data errors, inconsistent time periods, and erroneous assumptions.

Another reason for the lack of controversy is that the legislation regulated matching procedurally but not substantively. The matching amendments did not raise or resolve any legal questions about whether or when matching programs could be justified as a routine use under the Privacy Act. Over time, other legislation authorized or expressly required agencies to conduct many computer matches, so the need to justify routine uses under a compatibility standard disappeared in large part. If a statute required a disclosure, then the disclosure was effectively compatible as a matter of law. For other matches, the adoption of routine uses continued without much question.

The closest the matching amendment came to addressing the routine use issue came in section 9 of the law, a section not codified in the Privacy Act of 1974. The "rules of construction" stated that nothing in the matching amendments could be construed to authorize computer matching not otherwise authorized by law.[97] Congress was careful to say that the amendments did not authorize matching, but it left the legal question about routine uses otherwise unresolved. Computer matching continued on as it did before. The computer matching amendments succeeded politically because they were modest and procedural, avoiding attacking matching directly.

---

[95] See, e.g., Computer Matching and Privacy Protection Act of 1988, Report of the House Committee on Government Operations, 100th Cong., 2d Sess. at 6 (House Report 100-802) (report to accompany H.R. 4699).

[96] One consequence of the errors found in early matching was efforts to improve the quality of data used in matching. Over time, agencies worked to verify and correct Social Security Numbers that created incorrect matches and to more carefully align dates so that record being matching covered the same periods. These efforts, by reducing unfair matching results, may have helped to damp down some opposition to matching.

[97] Public Law 100-503, § 9, Act of Oct. 18, 1988, 102 Stat. 2514, http://uscode.house.gov/statutes/pl/100/503.pdf, 5 U.S.C. § 552a note.

Even as debates about computer matching continued, technology and administrative practices moved on. Agencies started using front-end verification, which seeks to certify the accuracy and completeness of personally identifiable information at the time an individual applies for government benefits, employment, or services. The Office of Technology Assessment found that front-end verification created a de facto national database covering most Americans and led to the establishment of individual databases for verification purposes and to the connection of these databases through online telecommunication linkages.[98] Front-end verification offered some similar and some different privacy challenges than computer matching, but congressional interest waned after passage of the matching amendments, and those challenges went unexplored. Arguably, the direct and permanent linkage of disparate databases is a worse outcome for privacy than the occasional exchange of information for matching. On the other hand, front-end verification reduced the sharing of less personally identifiable information between disparate programs because it shared only information about program applicants. This is arguably a more favorable outcome for privacy.

Professor Regan gets the last word here. She wrote: "Catching 'welfare cheats' was a more popular symbol than fear of Big Brother."[99] That remained true from the first matching program until and beyond passage of the computer matching amendments.

3. Akaka Bill

Senator Daniel Akaka's bill, Privacy Act Modernization for the Information Age Act of 2011, proposed a new definition for *routine use*.

> the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which, as determined by the agency, is compatible with the purpose for which it was collected and is appropriate and reasonably necessary for the efficient and effective conduct of Government.[100]

The core of the definition is the compatibility test in current law, but it adds several new ideas. First, it requires the agency to determine the purpose of the disclosure. It is not entirely clear what determining the purpose means in practice, although another part of Akaka's bill required a system notice to include *any purpose for which the information is intended to be used, including each routine use*.[101]

Second, Akaka's routine use must be both appropriate and reasonably necessary for the efficient and effective conduct of Government. If a disclosure is not compatible with the purpose for which the record was collected but is otherwise appropriate and reasonably necessary for efficient and effective government, then presumably the disclosure would not be allowed. This raises the same issue that arose with computer matching, where disclosures for matching seemed unrelated to the original purpose but served other governmental interests and attracted significant political support. For

---

[98] Office of Technology Assessment, *Electronic Record Systems and Individual Privacy* chapter 4 (1986), https://ota.fas.org/reports/8606.pdf.

[99] Priscilla Regan, Legislating Privacy 92 (1995).

[100] S.1732, 112th Cong., 1st Sess. § 2(a)(3) (2011), https://www.congress.gov/bill/112th-congress/senate-bill/1732.

[101] Id. at § (d).

computer matching, the disclosures proved impossible to resist. The Akaka standard does not clearly resolve this tension, a tension that is ultimately at the core of the compatibility problem.

4. Europe

The original 1995 European Union Data Protection Directive[102] addresses the same problem about defining allowable disclosures that the Privacy Act of 1974 did twenty-one years earlier. The 2016 General Data Protection Regulation came along twenty-one years after the Directive and starts with the same basic solution as the Directive.[103]

The Directive's main provision addresses *further processing*, a concept that includes disclosures to third parties:

> 1. Member States shall provide that personal data must be: ***
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.[104]

The Directive uses a compatibility standard, but it reverses the standard the Privacy Act uses. Rather than allowing a disclosure ("further processed") that is *compatible* with the purpose for which the record was collected as the Privacy Act does, the Directive allows disclosure as long as the disclosure is *not incompatible* with the original purpose for processing. This double negation makes a difficult standard harder to fathom. The Article 29 Working Party – the group of EU data protection authorities established under the Directive – concludes:

> By providing that any further processing is authorised as long as it is not incompatible (and if the requirements of lawfulness are simultaneously also fulfilled), it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis, as will be shown below.[105]

---

[102] Council Directive 95/46, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31995L0046:en:HTM, (hereinafter Data Protection Directive).

[103] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1551129473269&uri=CELEX:32016R0679 (hereinafter GDPR).

[104] Data Protection Directive at Art. 6.

[105] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation at 21 (2013) (00569/13/EN), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. (hereinafter Article 29 Purpose Limitation Opinion).

The need for *flexibility* and a *case-by-case* determination is consistent with the history of the routine use in the Privacy Act of 1974. The need for both clear standards and flexibility is the core of the *compatibility problem*, and Europe does not have a word formula that solves the problem.

There is more history here. The Article 29 Working Party discussed the background from the European Convention on Human Rights, the Council of Europe's Convention 108 for the Protection of Individuals with regard to automatic processing of personal data, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[106] That history, which clearly informed the choices made by the EU, will not be reviewed here. High-level principles have their place, but devising a statutory standard for a diverse group of data controllers to apply in a wide variety of circumstances is different and more difficult. Operationalizing a high-level principle is a clear challenge for any privacy law.

In analyzing the EU policy in this context, it is important not just to focus on the compatibility standard but to pay attention to *purpose specification* as well. As the Article 29 Working Party observes: "Specification of purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation."[107] Further, the Working Party states expressly that "purpose specification and compatible use are essential principles in the system of data protection."[108]

The focus on purpose specification is an important difference between the EU approach and the Privacy Act of 1974. The Privacy Act says plainly and flatly that a routine use must be compatible with the purpose for which a record was collected. There is no further explanation. The Act requires publication of a system of record notice describing details about the system, but the notice does not even require agencies to state the purpose of processing.[109]

In contrast, the EU directive states that personal data must be collected *for specified, explicit and legitimate purposes*. These three adjectives narrow and refine the notion of *purpose*. The Article 29 Working Party document offers five pages explaining how to understand and apply these three adjectives.[110] By contrast, under the Privacy Act, *purpose* attracts little attention, perhaps because there are no directions or standards for defining *purpose*.

To be sure, the Article 29 Working Party document also offers pages of discussion on how to assess compatibility.[111] The argument here is not that the Directive's focus on purpose fully solves the challenge of defining compatibility, only that it provides more express context for making compatibility determinations.

---

[106] Article 29 Purpose Limitation Opinion at 6-11.

[107] Id. at 4.

[108] Id. at 11.

[109] 5 U.S.C. § 552a(e)(4). Over time, the practice of including a purpose section in the system of records notice became commonplace. The level of detail in that purpose section varies considerably from system notice to system notice. The purpose description is much more likely to be a broad statement rather than a specification of all relevant purposes.

[110] Article 29 Purpose Limitation Opinion at 15-20.

[111] Id. at 20-27.

Those determinations are not necessarily easy to make or made consistently by EU member states. The Article 29 Working Party found divergent applications of the policy as implemented by the member states under the Directive.

> The divergences touch upon several aspects of the concept. Member States apply different tests to analyse the notions of purpose specification and incompatible use. In some countries, specific rules may apply to the public sector. In others, purposes may sometimes be defined in very broad terms. The approaches in the different Member States also vary as to how the purposes are made explicit, for example, whether specification of purpose is required in the notification to the data protection authority or in the notice to the data subject. The rules concerning the change of purpose, including for research and statistical purposes, also vary considerably, as they do in terms of the requirement of safeguards for these specific uses.[112]

There are further lessons from the 2016 European General Data Protection Regulation (GDPR), the data protection instrument that superseded the 1995 Directive. The GDPR starts with the same language – more or less – as the Directive. GDPR provides in relevant part:

> 1. Personal data shall be: ***
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').[113]

Both the Directive and the GDPR address the subject of processing for historical, statistical or scientific purposes by stating expressly that further processing for these purposes is not considered as incompatible with the original purpose. The GDPR also includes processing for archiving in the public interest. All of these disclosures might raise questions in many contexts about whether they meet – or need to meet – any compatibility test. The express provision in the GDPR (as well as the earlier Directive) cut off the need for debate with a broad, affirmative conclusion. In other words, these activities are generally favored in society's interest as to be allowed without any compatibility testing at all.[114]

---

[112] Id. 10 (footnote omitted).

[113] GDPR at Art. 5.

[114] The GDPR provides additional details on public interest processing. GDPR at Art. 89, (Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).

Sidebar: Public Interest Disclosures

The Article 29 Working Party addressed the ambiguity about compatibility in the Directive's "exceptions" for public interest processing. Are the blanket authorizations for further processing merely exceptions to the rule or do they offer a gloss on the meaning of compatibility? The Working Party offers its opinion:

> It is not clear from the text of Article 6(1)(b) alone whether this specific provision should be seen as an exception to the general prohibition of incompatible use in order to give a privileged position to 'historical, statistical or scientific purposes' or as a specification of the general rule, while not excluding that other cases could also be considered as 'not incompatible'. The analysis in this Opinion firmly supports this second view: the specific provision could give rise to more general criteria for compatibility (e.g. potential impact on the data subject, and appropriate safeguards).[115]

It is likely that the public interest provision resulted from strong lobbying by the historical, statistical, and scientific communities. This is not to suggest, however, that the public interest exceptions are inappropriate. The Working Party saw the exceptions as applications of the general rule.

The Privacy Act took a similar step with the inclusion of so-called statutory routine uses that allow disclosure from all systems of records for nine stated purposes.[116] These statutory routines uses solve a variety of problems. Some address disclosures that every agency faces (e.g., disclosures required by the Freedom of Information Act or disclosures to the National Archives for historic preservation). Two of the statutory routine uses address disclosures for statistical purposes, one for the Census Bureau and one covering non-identifiable records transferred for statistical research. The first of these statistical disclosures covers only one of the many statistical agencies in government, and the second is useless in practice. Another statutory routine use covers disclosures for law enforcement purposes, but it requires a written request from the head of the agency seeking the record and is thus too narrow to cover all necessary disclosures for law enforcement. Two of the statutory routine uses protect congressional interests by allowing disclosure to Congress, its committees, and the General Accounting Office (now Government Accountability Office), an agency that serves among other things as an auditor subject to congressional influence. Overall, the statutory routine uses are a mixed bag, solving some problems, but leaving other problems for agencies to resolve through additional routine uses. Whether these universally allowable disclosures should inform how to interpret *routine use* has rarely, if ever, been explored. Regardless, there is no express *public interest* standard for Privacy Act disclosures.

Evidence that the Directive's standard for further processing left something to be desired is found in new language added by the GDPR. Article 6 of the GDPR adds almost 200 words to guide the determination of what is legitimate processing for a purpose other than the purpose of collection:

> 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
>
> (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
>
> (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
>
> (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
>
> (d) the possible consequences of the intended further processing for data subjects;
>
> (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.[117]

A few observations about this language may be useful here. First, the GDPR makes clear that further processing with data subject consent and processing in accordance with law are both allowable. Under the Privacy Act, disclosure with consent is always allowable,[118] but the status of disclosures allowed or

---

[115] Article 29 Purpose Limitation Opinion at 13.

[116] 5 U.S.C. § 552a(b)(4)-(12).

[117] GDPR at Art. 6. See also GDPR at recital 50 ("The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal

required by other legislation is unaddressed. Second, purpose and context are important in assessing further processing for the GDPR. Under the Privacy Act, purpose is the only factor. Third, the additional GDPR language helps in ascertaining whether further processing "is compatible with" the original purpose. The earlier language in Article 5 retains the double negation ("not to be considered to be incompatible with the initial purposes") used in the Directive. It is not immediately apparent how to reconcile a *not incompatible* with a *compatible* or even if there is any real difference.

I suggest that this review shows why the compatibility problem is not easy to solve.[119] Europe had two bites at the compatibility apple, and while it provided more words the second time around, it did not find a bright-line test. I doubt that such a test exists. Any assessment of compatibility applicable in a general-purpose privacy law will necessarily call for consideration of multiple factors that bear on the decision to allow or not allow further processing or further disclosure. While assessments can be channeled in certain directions and measured on various scales, a final decision in hard cases typically requires human judgment. Is a disclosure the right thing to do under all the circumstances? Judgments here are not always hard, and most people likely would reach the same result much of the time, but the details may matter a lot. Still, difficult or controversial choices will arise, and judgments may differ. We must recognize as well that the agencies making the judgments may have conflicting interests.

When substantive criteria are difficult to apply, it is sometimes useful to require a process to be followed. Recall, for example, that the Privacy Protection Study Commission proposed certification by a designated official. Many recent practices in the privacy realm rely as much on process and procedure as standards. Privacy officers, privacy impact assessments, and privacy by design are examples of responses to privacy that rely at least in part on process and procedure rather than substantive line-drawing. Legislation cannot cover all contingencies or establish standards to be applied ministerially. Legislation can, however, state the factors that decisionmakers must consider when writing and approving further disclosures. Legislation can require that allowable disclosures be more specifically and more narrowly defined. Legislation can require public input as well. Legislation can provide a method for challenging choices and for making decision makers accountable.

---

data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.").

[118] 5 U.S.C. § 552a(b) ("except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains").

[119] The same problem arises with the efforts in California to implement the California Consumer Privacy Act, [Cal. Civ. Code §§ 1798.100–1798.199, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=. For a description of some of the attempts to apply the law's purpose limitation principle, see Bret Cohen & John Williams, What does the CCPA's 'purpose limitation' mean for businesses? (Sep. 2020), https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses/. That short article discusses briefly earlier efforts by the FTC to address purpose specification. The newly approved referendum (Proposition 24) enacting the California Privacy Rights Act of 2020 presents the same issues for resolution.

The USA FIPS Act does not use the term *routine use* but proposes a new term, *agency designated disclosure*. The bill also adjusts the standards and adds a series of requirements intended to make allowable disclosures easier to understand and potentially narrower in scope. The section-by-section discussion later in this report explains the specifics.

C. Privacy Act Exemptions

1. Introduction

The Privacy Act of 1974 has two classes of labeled exemptions plus two unlabeled provisions that function as limited exemptions. The labeled exemptions (so-called (j) and (k) exemptions) are the general (j) exemptions,[120] which come in two types, and the specific (k) exemptions[121] with seven types.

---

[120] 5 U.S.C. § 552a(j) ((j) General Exemptions. – The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is – (1) maintained by the Central Intelligence Agency; or (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, 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.

[121] Id. at (k) (Specific Exemptions. – The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

An agency seeking the use a (j) or (k) exemption must first go through a rulemaking before it can invoke the exemption in any given instance, but the two unlabeled exemptions do not require a rulemaking or any predicate.

The first provision that acts as a limited exemption allows an agency to withhold from individual access "any information compiled in reasonable anticipation of a civil action or proceeding."[122] The Department of Justice Guide to the Privacy Act describes it as "sometimes mistakenly overlooked" because it does not appear with the other exemptions.[123] This (d)(5) exemption is often called the *attorney work product* exemption. It is comparable to, if not identical with, the attorney work product exemption that is part of Exemption 5 of the FOIA. The FOIA exemption protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."[124] There does not appear to be any particular controversy over the need to protect attorney work product information, although there may be questions in any given application of the principle whether a particular document qualifies as work product.

The second limited exemption covers records transferred to the National Archives, and there are two subtypes here.[125] Records sent by an agency for storage in an Archives records center remain subject to the Privacy Act and are the responsibility of the agency that sent the records. This remains an unobjectionable result, but it may not need a statutory provision to achieve it. An agency is responsible for its own records no matter the storage facility.

The Archives subsection distinguishes records stored by the Archives from records accepted by the Archives for historic preservation.[126] The latter records, the second type of records addressed by the Archives limited exemption, are mostly exempt from the Privacy Act. The Archives must still publish a notice about the records. The publication provision duplicates language in 44 U.S.C. § 2019 that requires the Archivist to prepare and publish "inventories, indexes, catalogs, and other finding aids or

---

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.").

[122] Id. at (d)(5). The exemption effectively exempts the records from amendment requests as well.

[123] Department of Justice, Privacy Act Overview 278 (2015), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

[124] 5 U.S.C. § 552(b)(5).

[125] 5 U.S.C. § 552a(l).

[126] The two paragraphs of § 552a(l) that address records accepted for historic preservation distinguish between records transferred prior to the effective date of the Privacy Act of 1974 and those transferred after the effective date. The distinction seems either obsolete or unnecessary today.

guides to facilitate" use of transferred records.[127] The objectives of the historic preservation provision can be readily met with simpler language.

For both general and specific exemptions, an agency must go through a formal rulemaking to apply an exemption to a specific system of records. This contrasts with the exemptions in the Freedom of Information Act, which agencies may use when appropriate without any preconditions in responding to a request for agency records. The *attorney work product* exemption in the Privacy Act is available in the same way as other FOIA exemptions.[128] If a record in a system of records is attorney work product, the record may be withheld without any prior rulemaking or other action by the agency, and the exemption is available for all systems of records.

In its 1977 review of the Privacy Act, the Privacy Protection Study Commission found that the exemptions narrow the scope of the law's application and unduly frustrate achievement of the Act's basic objectives.

> While one can agree with the basic public-policy determination that some Federal agency records should not be subject to all of the Privacy Act's requirements, lest ongoing law enforcement investigations or legitimate national security interests be jeopardized, it nonetheless seems clear that the exemption provisions currently in the Act unnecessarily narrow its scope of application and thus unduly frustrate the achievement of its basic objectives. The Secret Service, for example, has had to exempt its entire "Criminal Investigation Information System" [41 F. R 45437 (October 14, 1976)] in order to exempt any part of it, even though many of the records in the system could be (and, under the Freedom of Information Act, often are) open to the individuals to whom they pertain; could be susceptible to correction and amendment without undue burden on the agency; and could be maintained with relatively strict procedures for assuring their accuracy and relevance when they are disclosed to third parties. In particular, one of the four categories of information in the system – records "consisting only of identifying data and notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status" – could be brought within the full scope of the Act without unreasonable difficulty. Such records, largely derived from public records, are unlikely to jeopardize ongoing investigations if disclosed to the individuals to whom they pertain and if inaccurate, but used to make a decision about an individual, either by the Service itself or by another agency, could be the cause of substantial harm to the individual.
>
> Agencies not ordinarily thought of as investigative or law enforcement agencies are often in the same position as the Secret Service. The Federal Trade Commission's "Investigational, Legal, and Public Records" system in many respects parallels the Secret Service's Criminal Investigation Information System, but it too has been exempted in its entirety. [41 FR 39719 (September 15,1976); 16 C FR. 4.13][129]

---

[127] 44 U.S.C. § 2019, https://www.law.cornell.edu/uscode/text/44/2109.

[128] 5 U.S.C. § 552(b)(5).

[129] Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment 8 (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

The PPSC proposed abandoning the systemic exemptions in the Privacy Act and using FOIA-like exemptions so that there would be "one set of standards for determining when access will *not* be granted."[130] The PPSC approach retained most of the (k) exemptions, "although in a form which permits them to be invoked only for the purpose of restricting individual access."[131]

For the (j) exemptions, applicable to all Central Intelligence Agency records or by any agency whose principal function is any activity pertaining to criminal law enforcement, the Commission's approach would not allow complete exemptions from requirements such as sharing corrections of records with prior recipients, reporting on new systems of records, and assuring the necessity and relevance of the information they collect.

As a rule, it is safe to assume that any agency establishing an exemption for a system of records invoked all available exemptions for that system. There are some exceptions to this assumption, but they are rare. One noteworthy exception to the rule comes from the Central Intelligence Agency and is discussed below.

2. Issues

a. The travelling exempt record problem

An agency that wants to invoke one of the Act's (j) or (k) exemptions must undertake a rulemaking that applies an exemption to a particular system of records. However, at times, one agency shares a record exempt under one system of records with another agency. The shared records in the hands of the receiving agency may end up in a different system of records for which the receiving agency established no exemption.

The structure of the Act's exemptions creates a gap in protection for exempt records as the Act's drafters did not provide a solution. The 1974 OMB Guidelines addressed the issue by focusing on the need to protect the contents of an exempt record. However, OMB did not squarely address the problem of an exempt record in a non-exempt system.

> Agency records which are part of an exempted system may be disseminated to other agencies and incorporated into their non-exempt records systems. The public policy which dictates the need for exempting records from some of the provisions of the Act is based on the need to protect the contents of the records in the system – not the location of the records. Consequently, in responding to a request for access where documents or another agency are involved, the agency
> receiving the request should consult the originating agency to determine if the records in question have been exempted from particular provisions of the Act. A copy of the request may be forwarded to the originating agency for handling of its documents where such a procedure would result in a more rapid response to the request for access but the agency receiving the request remains responsible for assuring a prompt response. Agencies which elect to invoke exemptions are encouraged to adopt procedures similar to those prescribed by the Act wherever

[130] Id. at 123.

[131] Id. at 124.

appropriate.[132]

A problem here is that the Act seemingly has two conflicting objectives. One is to require that agencies complete a rulemaking in order to exempt records from the Privacy Act. The other objective is to allow agencies to protect records that qualify for available exemptions. A new law needs to resolve the conflict once and for all. If it is possible to have at least some FOIA-like exemptions that do not require notice and rulemaking, then the problem will diminish. However, if there is no rulemaking, there might be no public notice and opportunity to comment. The draft bill finds a different way to accomplish both objectives.

The courts allow agencies to continue to apply an exemption when an agency transfers a record from an exempt system to a non-exempt system.[133] This appears to be a less than ideal long-term solution.

It would be appropriate for an agency notice of an agency activity affecting privacy to disclose the presence of exempt information in some manner. If an agency activity is likely to have exempt information – and this will be known in many cases – that information can be included in the agency notice of the A3P. The goal of the notice is to tell individuals that some records may be exempt, but not in a way that would prevent an agency from claiming an exemption if an exempt record (from another internal activity or another agency) appeared without notice.

How does an agency that receives an exempt record from another agency know that the record is exempt? If agencies follow a consultation procedure as suggested in the 1975 OMB Guidelines, that would address the problem. However, another alternative is to require an agency transferring an exempt record to another agency to expressly mark the record as subject to an exemption claim and thereby provide explicit notice to the receiving agency. That is the approach taken in the draft.

b. Classified information

The Privacy Act's (k)(1) exemption allows an agency to exempt a system of records if the system is "subject to the provisions of section 552(b)(1)" of title 5. That provision exempts from mandatory disclosure under the FOIA any information "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order."[134]

---

[132] Office of Management and Budget, Privacy Act Guidelines 82-3, 40 Fed. Reg. 28948 (July 9, 1075), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

[133] See *Doe v. FBI*, 936 F.2d 1346, paragraph 51 (D.C. Cir. 1991) ("information contained in a document qualifying for subsection (j) or (k) exemption as a law enforcement record does not lose its exempt status when recompiled in a non-law enforcement record if the purposes underlying the exemption of the original document pertain to the recompilation as well." https://openjurist.org/936/f2d/1346/doe-v-federal-bureau-of-investigation-doe.

[134] 5 U.S.C. § 552(b)(1).

Given that classified information is always subject to withholding, there is no reason to require a rulemaking to protect it from disclosure. Thus, classified information could be exempt from the access and amendment provisions of the Act in the same way that attorney work product is exempt.[135]

With one exception, all the (k) exemptions relate in some way to access and amendment. The (k) exemptions allow for a system of records to be exempted from the requirement to disclose accounting records,[136] from the requirement to comply with the access *and* amendment provisions,[137] from the obligation to disclose in a system of records notice rules and procedures for providing access and amendment rights and sources of records,[138] and from the requirement to publish agency rules regarding access and amendment rights.[139] For classified information, the basic publication of a notice for an A3P can cover all access and amendment issues. The remaining exemption available today is from the requirement in (e)(1) to maintain only relevant and necessary information. It is appropriate to continue that exemption as well.

c. Confidential Sources and the (e)(1) Requirement

If restrictions on access and amendment rights can be covered through the notice as part of a A3P notice and comment rulemaking, there are still other issues raised by the (k) exemptions that need discussion. For example, several of the (k) exemptions allow agencies to protect against the identification of confidential sources of information. There is little argument that protecting confidential sources is valuable. This need might be covered by simply providing in the general notice requirement and in the agency rules that sources that must be identified do not include "any sources for classified records" or perhaps "any classified sources for classified records." Any access and amendment exemptions can be addressed in agency rules, as can access to accounting records.

A different problem arises because systems of records exempt under the (k) exemptions may also be exempted from the *relevant and necessary* provision of the Privacy Act:

> (e) Agency Requirements. Each agency that maintains a system of records shall – (1) 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.[140]

There is no apparent reason for providing an exemption from the *relevant and necessary* provisions for the (k)(4) exemption for statistical records. The maintenance of statistical records raises no concerns about the scope of records kept. The testing and examination exemption is so narrow that the *relevant and necessary* language is unnecessary.

---

[135] The existing attorney work product exemption is sufficient to protect government interests even though attorney work product is not expressly exempt from the other provisions relating to access and amendment that are available through the (k) exemptions.

[136] 5 U.S.C. § 552a(c)(3).

[137] Id. at (d)

[138] Id. at (e)(G), (H), & (I).

[139] Id. at (f).

[140] Id. at (e)(1).

This leaves five (k) exemptions to be considered regarding a need for an exemption from the (e)(1) requirement. The (k)(5) exemption covers investigatory material compiled solely for determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information. The (k)(7) exemption covers evaluation material used for determining promotion in the armed services. Both of these exemptions have a significant limitation. The exemption applies only to the extent that disclosure would reveal the identity of a confidential source. All other information is available to the data subject upon request.

The (k)(2) exemption covers investigatory material compiled for law enforcement purposes other than material maintained by an agency or component that performs as its principal function any activity pertaining to the enforcement of criminal laws. When collecting information for any law enforcement activity whether criminal or civil, it is difficult to know at the time of collection what will be relevant and necessary to an investigation. The need an exemption from the *relevant and necessary* requirement for (k)(2) activities remains strong.

Similarly, there is a good case for maintaining an exemption from the *relevant and necessary* standard for the (k)(3) exemption covering protective services for the President and others. The nature of protection services makes it difficult to apply a *relevant and necessary* rule.

The (k)(6) exemption, covering, covers testing and examination requirements for federal service, does not appear to require an exemption from the (e)(1) requirement.

d. (j)(1) exemption

The (j)(1) exemption covers all systems of records maintained by the Central Intelligence Agency.[141] The exemption is available for all CIA systems regardless of their content or sensitivity. The Act requires a published explanation for exempting a CIA system.[142]

For each of its most recently published 41 systems of records, the CIA claims an exemption in this fashion:

> Certain records contained within this system of records may be exempted from certain provisions of the Privacy Act (5 U.S.C. 552a) pursuant to 5 U.S.C. 552a(j)(1), (k), and (d)(5).[143]

This same claim for exemption is included even for CIA-10, a system of records for parking records.[144]

Still, it is noteworthy that the CIA claims an exemption only for "certain records contained within this system of records" and not for all records automatically.

---

[141] 5 U.S.C. § 552a(j)(1).

[142] Id. at (j) ("At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.").

[143] Privacy Act Issuances (2019), https://www.govinfo.gov/content/pkg/PAI-2019-CIA/xml/PAI-2019-CIA.xml.

[144] Id at https://www.govinfo.gov/content/pkg/PAI-2017-CIA/xml/PAI-2017-CIA.xml#cia10.

Further, the CIA rulemaking covering the exemptions indicates that application of the exemptions is narrower in practice.[145] The rule limits the reasons an exemption would be employed in practice. The provision that exempts CIA systems of records from the access and amendment rights in subsection (d) of the Act applies only those portions of all systems of records maintained by the CIA that:

> (1) Consist of, pertain to, or would otherwise reveal intelligence sources and methods;
> (2) Consist of documents or information provided by any foreign government entity, international organization, or, any United States federal, state, or other public agency or authority; and
> (3) Consist of information which would reveal the identification of persons who provide information to the CIA Inspector General.[146]

In principle, this stated policy of limited application of the exemptions only when it serves a specific defined purpose is appropriate and commendable. The effect is to suitably and significantly narrow the breadth of the statutory exemption. It suggests that the (j)(1) exemption is broader than is necessary. The CIA was under no obligation to narrow the exemption through its rulemaking, but it did so anyway.

I gave serious consideration to including the CIA regulatory limits in the statute, but I rejected the idea. First, the USA FIPS Act gives rights to foreign nationals whereas the Privacy Act covers only citizens and resident aliens. With the broader class of individuals with rights, the CIA might not choose to apply the limitations as it does today. Second, the CIA exemptions as adopted probably principally serve to support the rights of CIA employees. That is a surmise, but the idea of expressly providing rights to intelligence agency employees has some attractions. In the end, however, I was concerned about how to define *employee* for this purpose. An intelligence agency like the CIA likely hires individuals to work through a wide variety of relationships. Trying to figure that out would be difficult.

Another (j)(1) issue is that the CIA is not the only intelligence agency. One can guess that the CIA exemption arose in the first place because of a specific objection made during negotiations between the House and Senate over their respective versions of the Privacy Act, negotiations that took place near the final congressional adjournment date. The political choice available was likely exempt the CIA or not have a bill. Since 1974, the number of formally recognized intelligence agencies broadened. Extending the same exemption to all intelligence agencies or intelligence components of agencies is both reasonable and politically compelling. The bill does this.

Rather than narrow the intelligence exemption, the bill takes a different tack. A new provision encourages – but does not require – agencies with exempt records to waive the exemption through a variety of mechanisms, either systemic or on a case-by-case basis. Whether intelligence or other agencies will take up this invitation is unknown, but the CIA precedent is encouraging.

---

[145] 32 C.F.R. Part 1901, https://www.ecfr.gov/cgi-bin/text-idx?SID=9a6b5d672d5cf0462842c381f2bf2b52&node=pt32.6.1901.

[146] Id. at § 1901.62(d).

Defining what is an intelligence agency turns out to be simple. Executive Order 12,333 defines the Intelligence Community and agencies within the Intelligence Community.[147] There is no reason to reinvent this particular wheel, and the bill just cites the Executive Order.

e. (j)(2) exemption

The (j)(2) exemption is for an agency or agency component that performs as its principal function any activity pertaining to the enforcement of criminal laws. The full exemption provides that it can be applied to any system of records –

> maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, 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.[148]

The (j)(2) exemption is much more specific than the (j)(1) exemption in that the (j)(2) exemption specifies the type of information that can qualify. The (j)(1) exemption applies broadly to any CIA system of records and any information in those systems. There is no evidence that the (j)(2) categories of exempt records need to be revisited. An agency claiming a (j)(2) exemption, must explain reasons for claiming the exemption when publishing its description of an A3P.[149]

The (k) exemptions already discussed mostly allow agencies to exempt activities from all aspects of the Act's access and amendment requirements. As discussed, the only non-access/amendment exemption available is the provision in (e)(1) regarding the maintenance of only relevant and necessary information.

The (j) exemptions are much broader than the (k) exemptions. A system of records subject to the (j) exemptions can be exempted from all provisions of the Act *except* the limits on use and disclosure;[150] the requirement to maintain and retain an accounting of disclosures;[151] the publication of a system of records notice;[152] the requirement to make reasonable efforts to assure that records are accurate,

---

[147] Executive Order 12,333, United States Intelligence Activities at Part 3.4(f) (1981), https://www.archives.gov/federal-register/codification/executive-order/12333.html.

[148] 5 U.S.C. § 552a(j)(2).

[149] Id. at (j).

[150] 5 U.S.C. § 552a(b).

[151] Id. at (c)(1) & (2).

[152] Id. at (e)(4)(A) through (F). An agency using the (j) exemption can exempt a system of records from the notice requirements in (G) & (H) that related to access and amendment, and that makes sense because the system can be

complete, timely, and relevant for agency purposes prior to disseminating a record to any person other than an agency;[153] the prohibition against maintaining records about how an individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the data subject, or unless pertinent to and within the scope of an authorized law enforcement activity;[154] the requirement to establish rules of conduct for those involved in the processing of records;[155] the requirement to maintain security safeguards;[156] and the requirement to publish a notice of a new routine use.[157] A (j) system can also be exempted from the civil remedies[158] but not from the Act's criminal penalties.[159]

It is a reasonable assumption that the parts of the Act applicable to systems of records subject to the (j) exemptions should continue to apply in a new law. A more complex question is whether all of the requirements from which (j) systems are exempt are still justifiable. What follows here is a discussion of each provision of the Act from which a (j) system of records can be exempted.

(c)(3) & (4): These provisions relate to accounting for disclosures, requiring an agency to make accounting records available to the data subject and to require the agency to inform those to whom a record was disclosed about any correction or dispute. Given that (j) systems are exempt from data subject access and amendment, continuing to allow an exemption from these two requirements makes sense.

(e)(1): This provision allows the maintenance of 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. The argument for this exemption is that both intelligence activities and criminal investigations need more leeway in standards for the maintenance of personally identifiable information related to an agency activity and that it is difficult to know at the time of collection what will be relevant and necessary to an investigation. On the other hand, without the (e)(1) limit, an agency can arguably maintain any information without regard to relevance or necessity. Whether there is a middle ground here remains to be seen. Some other exemptions qualify the exemption with the phrase *to the greatest extent practicable*. Whether the use of this or another limiting standard would make an actual difference is uncertain.

(e)(2) This provision requires the collection of information from the data subject *to the greatest extent practicable* if use of the information may result in an adverse determination about and individual's rights, benefits, and privileges under federal programs. In a criminal law enforcement context, the need for this exemption still makes sense, although it is fair to ask whether the "to the greatest extent practicable" solves most or all law enforcement issues that might arise here. The same

---

exempted from the requirement to allow access and amendment. An exemption is also available for the requirement in (I) to disclose categories of sources of records.

[153] Id. at (e)(6).

[154] Id. at (e)(7).

[155] Id. at (e)(9).

[156] Id. at (e)(10).

[157] Id. at (e)(11).

[158] Id. at (g).

[159] Id. at (i).

is likely true for intelligence activities. Still, one could easily question the need for any exemption in routine personnel matters.

(e)(3): This provision requires giving an individual asked to supply information on the form used for collection information about the authority, purpose, routine uses, and effects of refusal. Here too, the exemption continues to make sense for criminal law enforcement activities and for intelligence activities (other than routine personnel activities). In both cases, giving affirmative notices to those asked to provide information would undermine the goals of information collection.

(e)(4)(G), (H), & (I): The first two of these exemptions allow an (j) system to avoid publishing portions of a system of records notice that describe access and amendment rights. Given the exemption from access and amendment for (j) systems, this makes sense. If notices include only a reference to agency rules for access and amendment, however, then the issue can be addressed in the rules rather than in the notice. The exemption from (I) allows an agency to avoid publishing a description of the categories of sources of records. That makes sense for both types of (j) exemptions, but many categories of unclassified sources could probably be identified generically with no consequence.

(e)(5): This requirement obliges agencies to maintain 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. An exemption for intelligence records continues to make sense. The argument for criminal law enforcement records seems weaker given that fairness in criminal law enforcement determinations is a reasonable goal, but it may be harder to impose a standard that should apply at the end of a law enforcement determination throughout the investigatory process.

(e)(8): This provision obliges an agency to notify an individual if that individual's record is made available to any person under compulsory process when the process becomes a matter of public record. This obligation is unlikely to ever attach to intelligence activities. For criminal law enforcement, given that the process became public, there may be no strong reason for an exemption other than administrative burden. Here too, the obligation may rarely, if ever, arise.

(f): The exemption from agency rulemaking in this subsection relates to access and amendment procedures. If the exemption from access and amendment is justified, then this exemption is arguably justified as well. Some courts, however, found the amendment exemption unavailable when the document in question had been made public.[160] Further, just because a record is exempt from access, an agency may choose to allow an individual access because the interests protected by the exemption do not arise. In those cases, the agency still needs rules and procedures. In the end, the exemption from having rules may not be necessary provided that the rules required under the draft bill recognize that access may not be granted in all cases.

(g): The exemption from the Act's civil remedies has been significantly controversial. It is one thing to say that an agency does not have to follow all privacy rules in all cases. It is something else to say that an agency cannot be held accountable in court for following what provisions do apply. The broad civil remedy exemption has not been welcomed by the courts, which have found ways to limit

[160] Department of Justice, Privacy Act Overview 287-88 (2015), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

the effect of the civil remedy exemption.[161] One idea is to limit the exemption so that it is available only to a record or activity for which an exemption applies. That would eliminate the implication that an agency is somehow unaccountable for compliance with any part of the Act, even those parts that apply notwithstanding the (j) exemption. In the end, the bill drops the civil exemption provision entirely. The policy is simple: agencies should be held accountable for complying with the Act.

(h): An exemption is available from the provision that addresses rights of minors and those declared incompetent. The exemption here is unnecessary. The issue of guardians is unlikely to arise, and even if it does, any available exemptions on individual rights would apply to guardians.

(j) & (k): Technically, (j) and (k) systems of records can be exempted from the (j) & (k) provisions. This makes little sense, and it is just a consequence of an exemption phrased as "everything but" the following provisions.

(l): The archival provision describes the status of records transferred to the National Archives. The continuing justification for this exemption is unclear.

(m): It is not clear why systems of records exempt under (j) need to be exempted from the requirement to cause the requirements of the Act to contractors. Even if an exempt system is as fully exempt from the Act as possible, there are still applicable requirements, perhaps most notably the limits on disclosure. It is hard to see a reason that agency contractors should not have to comply with those provisions of the Act that apply to the agency notwithstanding the application of a (j) exemption.

(n): It is not apparent why the limit on the sale of mailing lists cannot apply to records exempt under (j). In practice, the sale of lists by intelligence or law enforcement agencies is highly unlikely at best.

The remaining provisions of the Privacy Act for which exemptions are technically available were added to the Act in later years. It is likely that no one gave any thought to how these provisions related to the availability of exemptions under (j).

(o), (p), (q), (r), (u): These provisions all relate to computer matching activities. The exemption here is both okay and irrelevant, given that intelligence matching would not be covered by the provisions (except possibly for matches involving agency personnel) and that criminal law enforcement matching is for the most part outside the scope of the matching requirements.[162]

(t): This provision prevents an agency from treating the Privacy Act of 1974 as a (b)(3) statute under the FOIA and to prevent an agency from using the Privacy Act as a basis from withholding from an individual a record otherwise available under the FOIA. The language was a later amendment to the Privacy Act and, by happenstance, it technically fell under the scope of an exemption that applies to "everything but."

---

[161] Id at 288-93.

[162] 5 U.S.C. § 552a(a)(8)(B)(iii) ("matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, 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.").

(v): There is no reason for the availability of an exemption from the Act's provision that directs OMB to prescribe guidelines and provide assistance to agencies.

In the end, the proposed bill reformulates the exemptions in several ways. First, for the most part, it continues most existing exemptions, with the elimination of the possibility of an exemption from civil remedies being the most noteworthy general change. Second, it states all exemptions affirmatively and avoids language that says a system is exempt from *everything except* stated provisions. Third, it brings all provisions creating exemptions of any type into a single section of the bill. Fourth, it eliminates the need for special rulemaking, but public notice and comment will occur when agencies publish their A3Ps with exemption claims as part of the basic description. Fifth, it provides an express solution to the travelling exempt record problem. These are all improvements that will make exemptions clearer, provide for public notice and comment without a separate rulemaking, and hold agencies accountable. At the same time, the bill will continue protection of agency interests in confidentiality of federal operations.

Part IV. Section-by-Section Discussion of the Act

A. Title (Section 1)

Sec. 1. Short Title.

This Act may be cited as the "United States Agency Fair Information Practices Act (USA FIPS)".

The proposed title for the revised Privacy Act is the *United States Agency Fair Information Practices Act (USA FIPS)*. This title emphasizes the enduring importance of Fair Information Practices as the basis for privacy policy for the federal government. It also avoids the confusion that ensued by the lack of specificity in original title. The phrase "Privacy Act" was clear enough when that Act was new and among the first privacy laws enacted by any country. In later years when there were more privacy laws and when privacy matters grew more complex, references to the "Privacy Act" sometimes engendered confusion.

B. Findings and Purposes (Section 2)

Sec. 2. Findings and Purposes

(a) FINDINGS. – The Congress finds that –

(1) the right to privacy is a personal and fundamental right protected by the Constitution of the United States;

(2) the privacy of an individual is directly affected by the processing of personally identifiable information by Federal agencies;

(3) the increasing use of sophisticated information technology, data mining, artificial intelligence, and profiling of individuals and households greatly magnifies the harm to individual privacy that can occur from any unjustified, unnecessary, or careless processing of f;

(4) the opportunities for an individual to secure employment, insurance, and credit, to participate in social, political and economic marketplaces, and to achieve due process and other legal protections are endangered by any unjustified, unnecessary, or careless processing of personally identifiable information;

(5) in order to protect the privacy of individuals identified in information systems processed by Federal agencies, it is necessary and proper for the Congress to regulate the processing of personally identifiable information by the agencies;

(6) it is appropriate and important for Federal agencies to inform the public about the nature of agency personally identifiable information processing activities and for agencies to maintain accurate and current descriptions and records of those activities;

(7) reasonable implementation of the following principles of Fair Information Practices by Federal agencies will provide protections for individual privacy while allowing the Federal agencies to carry out their missions in an effective and efficient manner:

(A) the Principle of Collection Limitation provides that there should be limits to the collection of personally identifiable information, that the information should be collected by lawful and fair means, and that the information should be collected, where appropriate, with the knowledge or consent of the data subject;

(B) the Principle of Data Quality provides that personally identifiable information should be relevant to the purposes for which they are to be processed, and to the extent necessary for those purposes should be accurate, complete, and timely;
(C) the Principle of Purpose Specification provides that there must be limits to the processing of personally identifiable information and that the information should be processed only for the purposes specified at the time of collection and for compatible purposes;
(D) the Principle of Disclosure Limitation provides that personally identifiable information should not be disclosed except as provided under the purpose specification principle without the consent of the data subject or other legal authority;
(E) the Principle of Security provides that personally identifiable information should be protected by reasonable security safeguards against risks including loss, unauthorized access, destruction, use, modification, and disclosure;
(F) the Principle of Openness provides that the existence of record-keeping systems containing personally identifiable information be publicly known, along with a description of the record keeper, main purposes, uses, disclosures, policies, and practices for processing the information;
(G) the Principle of Individual Participation provides that individuals should have a right to see personally identifiable information about themselves and to seek amendment or removal of information that is not timely, accurate, relevant, or complete; and
(H) the Principle of Accountability provides that a record keeper should be accountable for complying with fair information practices.

(b) PURPOSE. – The purposes of this Act are to provide safeguards for the personal privacy of individuals by requiring Federal agencies, except as otherwise provided by law –
(1) to permit individuals to know how agencies process personally identifiable information;
(2) to restrict the use and disclosure of personally identifiable information to lawful, defined, and disclosed purposes;
(3) to permit data subjects to gain access to personally identifiable information pertaining to themselves in Federal agency records, to have a copy of the records, and to ask for amendment to the records;
(4) to process any record in a manner that assures that –
(A) the processing is for a necessary and lawful purpose;
(B) the personally identifiable information in the record is current and accurate for its intended use; and
(C) the processing provides adequate safeguards to prevent misuse of the information;
(5) to be subject to civil suit for any damages which occur as a result of willful or intentional action that violates any individual's rights under this Act; and
(6) to allow any person who believes that a Federal agency is not complying with this Act to ask the agency to bring its conduct into compliance.

The first finding is the same as a finding in the original Privacy Act.

The second finding is nearly the same as a finding in the original Privacy Act, with only a bit of rewording. I changed *personal information* to *personally identifiable information* here and elsewhere in the findings.

The third finding states a more general and more modern proposition than a somewhat comparable finding from the original law. The original finding is "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personally identifiable information."

The fourth finding is new, and like the third finding, addresses the consequences to individuals that can result from processing of personally identifiable information and from the use of information technology.

The fifth and sixth findings address the importance of regulating personally identifiable information processing and of informing the public about agency personally identifiable information processing activities. The fifth finding from the Privacy Act addresses the first point but not the second.

The seventh finding emphasizes the importance of implementing Fair Information Practices in a reasonable manner that protects privacy and that also allows agencies to operate effectively and efficiently. The finding includes a complete statement of FIPs.

The background in Part II of this report describes the origins and importance of FIPs. I included a statement of FIPs in this bill because it is important that American law recognize a single version of FIPs. American law already mentions FIPs in various places, but there is no statement of FIPs in U.S. Code.[163] One goal is to seek to end restatements and revisions of FIPs by federal agencies by having a congressional approved statement of the basic policy.[164] More history of FIPs, including many of the

---

[163] There are FIPs references in statute in: 50 U.S.C. § 3029(b)(5), http://www.law.cornell.edu/uscode/text/50/3029, (establishing a Civil Liberties Protection Officer within the Office of the Director of National Intelligence); in 42 U.S.C. § 2000ee-2, http://www.law.cornell.edu/uscode/text/42/2000ee-2, (requiring the Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board to have a privacy and civil liberties officer); 49 U.S.C. § 31306a(d)(1), establishing a national clearinghouse for controlled substance and alcohol test results of commercial motor vehicle operators that must comply with applicable Federal privacy laws, including the fair information practices under the Privacy Act of 1974, http://www.law.cornell.edu/uscode/text/49/31306a; in the Transportation Security Acquisition Reform Act, Pub. L. 113-245 § 3, 128 Stat. 2871, 6 U.S.C. 563a, (requiring the Administrator of the Transportation Security Administration to determine whether any security-related technology acquisition is justified by conducting an analysis that includes, among other things, a determination that the proposed acquisition is consistent with fair information practice principles issued by the Privacy Officer of the Department, https://www.law.cornell.edu/uscode/text/6/563a; The Cybersecurity Act of 2015, Pub. L. 114–113, div. N, title I, § 105, Dec. 18, 2015, 129 Stat. 2943, 6 U.S. Code § 1504(b)(3)(D) (providing that guidelines under the statute for retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government shall, among other things, be consistent with the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011), https://www.law.cornell.edu/uscode/text/6/1504. See also 6 U.S.C. § 142(a)(2), http://www.law.cornell.edu/uscode/text/6/142.

[164] See, e.g., Department of Homeland Security, Fair Information Practice *Principles*, https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles (italics added). Other agencies use FIPPs too.

restatements of FIPs by federal agencies, can be found in a FIPs history that I maintain on my website.[165]

This version in the bill originates with the highly influential version issued by the Organisation for Economic Cooperation and Development (OECD) in 1980.[166] This statement of practices is general enough to serve the purpose to describing the broad policy goals of a privacy law while not unduly limiting activities that require the processing of personally identifiable information. FIPs remain a reliable and essential foundation for privacy policy and legislation.

Since I made some modifications to the OECD FIPs, I offer an explanation. None of the language changes seeks any substantive alteration to the original policies. Some wording changes adjust the language of the OECD FIPs for a legislative format. Some language changes make FIPs gender neutral. The draft also uses *record keeper* rather *than data controller*.

First, I replaced *personal data* with the bill's defined term *personally identifiable information*. This is the only change in the Collection Limitation Principle.

Second, in the Data Quality Principle, I replaced *up-to-date* with *timely*.

Third, the Purpose Specification Principle is reworded generally. The major change is to the original language that subsequent use be limited to the original purposes "or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." The word *use* is difficult because it means *disclosure* in its original sense, but no longer has that meaning in modern privacy parlance. The concept of *incompatibility of purpose* raises what I call in the section above on Controlling Disclosure the *compatibility problem*. In place of the "not incompatible" language, I substituted "compatible purposes." I do not believe that this difference in wording is significant because none of these terms draws clear lines. That is a task for those who apply the principles.

Fourth, I renamed the Use Limitation Principle. It is now the Disclosure Limitation Principle. This change was essential because the bill defines use and disclosure in the modern privacy sense of the terms, a usage that postdates the original OECD version. This change does not seek to diminish the importance of limiting uses. That goal is fully met by the Purpose Specification Principle that information should be processed only for the purposes specified at the time of collection and for compatible purposes. There is, and always was, some overlap between these two principles.

Fifth, the Security Principle is unchanged but for the substitution of *personally identifiable information* for *personal data*.

Sixth, the Openness Principle is reworded somewhat, but the substance is the same as the OECD version.

---

[165] Robert Gellman, FAIR INFORMATION PRACTICES: A Basic History (2021, and occasionally updated), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf. This history sets out the full text of the original version of FIPs from the HEW Committee, as well as subsequent versions from other sources.

[166] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum.

Seventh, the Principle of Individual Participation confirms the right to see and to seek amendment of personally identifiable information. It offers less detail because the details seem out of place in a statement of principles and because a statement of basic rights implies (and the bill provides) due process with respect to these rights.

Finally, the Principle of Accountability is reworded, but the responsibilities of record keepers remain unchanged.

The bill includes six purposes that mirror in part the original statement of purposes from the Privacy Act of 1974.[167] The preamble to the statement of purposes in the bill is comparable to the original Act, and the six paragraphs that follow in the proposal set out requirements for federal agencies. In both statements, the first requirement relates to letting individuals know how agencies process PII.

The second purpose is totally restated because the original language set out an unrealistic goal. The original version says "permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent."[168] If that was a goal of the original Privacy Act, the Act was a failure because individuals have little control over use and disclosure of their PII. The provisions of the Act, especially the routine use provision and the internal agency use provision, allow agencies to avoid allowing individual control or participation in use and disclosure disclosures. The revision focuses broadly on the objective of restricting the use and disclosure of personally identifiable information to lawful, defined, and disclosed purposes.

The third purpose in both the original Act and the bill relates to individual rights of access and amendment. The two versions are substantially the same.

The fourth purpose in both versions is nearly identical, relating to processing information for appropriate purposes, with accuracy for its intended use, and with safeguards against misuse.

The fifth purpose discusses exemptions. There is no comparable purpose statement in the Privacy Act about exemptions, although the bill provides similar exemptions but in a significantly different way.

The sixth purpose in the original addresses enforcement of the Privacy Act by civil suit. There are two separate purposes in the bill relating to enforcement. One is similar to the original and references an individual's right to sue for a violation of rights under the Act. The second addresses enforcement in another way, referencing the new provision in the bill that provides for remedies for any person who believes that an agency is not complying with the law.

C. Definitions (Section 3)

Many of the definitions in the bill come from the existing Act, but there are some changes and some new terms.

1. Individual

[167] Public Law 93-579, 88 Stat. 1896, Act of Dec. 31, 1974, https://www.law.cornell.edu/uscode/text/5/552a (note).

[168] Public Law 93-579, § 2(b)(2).

> (1) INDIVIDUAL. –The term "individual" means a living individual and includes an individual acting as a sole proprietor.

The definition of *individual* makes several changes from existing law. First, it clarifies existing law that only living individuals have rights under the bill. That has been the general practice under the Act.

Privacy rights after death is a more complex subject than it was decades ago, in part because of the existence of electronic information maintained by numerous third-party record keepers inside and outside of government. The health privacy rule issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) originally required a HIPAA covered entity to protect the privacy interests of deceased individuals forever. In 2013, the Department of Health and Human Services changed the rule so that privacy obligations end fifty years after death.[169] The change is evidence that a forever rule has its shortcomings. So does the current policy, for that matter.[170]

When privacy rights continue after death, complex issues arise about the rights of heirs. With government records, questions about openness obligations arise.[171] If the bill changed current practice regarding privacy after death, these issues would have to be confronted. I do not believe that those issues are ripe for federal legislative attention at present, and any attempt to address them would likely require extended discussion and would be significantly controversial. These matters are best left for consideration at another time and in a broader context than just federal agency records. There has been some attention to and legislation proposed to address privacy rights after death, especially at the state level, but new laws remain rare.[172] The stakeholders in any privacy-after-death legislation are considerably different than those who care about federal agency privacy.

A second, less complex issue, resolved by the definition is the status of individuals who are sole proprietors.[173] The Privacy Act grants rights to individuals but not to legal persons. Sole proprietors fall in the middle. There is a split of authority on the question of sole proprietors, and agency practice varies.[174] I see no reason not to resolve this question in the bill by establishing a clear, uniform policy for all agencies. The bill grants sole proprietors the same rights as individuals.

---

[169] 45 C.F.R. § 164.502(f).

[170] There is no conflict here with health records subject to the Privacy Act of 1974 and to the HIPAA health privacy rule. The Privacy Act no longer applies to records of deceased individuals, but the HIPAA rule continues to protect the records for fifty years.

[171] When a public figure dies, it is common practice for reporters and others to use the Freedom of Information Act to ask for agency records about that public figure. FBI records are often sought. The FOIA policy is that the privacy interests protected by that law end at death. The issue is somewhat muddled because in several cases, the courts recognized a privacy interest for survivors of deceased individuals. See *National Archives and Records Admin. v. Favish*, 541 U.S. 157 (2004) (death of Vince Foster), and *N.Y. Times Co. v. NASA*, 920 F.2d 1002 (D.C. Cir 1990) (en banc) (space shuttle Challenger). Both cases involved the death of public figures. Whether the courts would find that a privacy interest arises after the death of non-public figures is far from certain.

[172] See Uniform Law Commission, Revised Uniform Fiduciary Access to Digital Assets Act (2015), https://www.uniformlaws.org/committees/community-home?communitykey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=groupdetails.

[173] In the interest of full disclosure, I disclose here that in my role as a privacy consultant, I am a sole proprietor.

[174] See generally Department of Justice, Overview of the Privacy Act of 1974 16-17 (2015), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

The third change made by the new definition grants privacy rights to all individuals. The Privacy Act of 1974 only grants rights to citizens and aliens lawfully admitted for permanent residence. Foreign nationals have no rights under the Privacy Act. During my years working on the House Subcommittee, I recall being told by those who worked on passage of the Act that the CIA insisted on excluding foreign nationals.

During informal discussions in 2011 between privacy advocates and Senate staff seeking to amend the Privacy Act of 1974, the issue of extending rights to foreign nationals arose. Senate staffers refused to consider it. The political problem was that it would allow Osama bin Laden to request his file, and the staffers did not want to confront that issue.

Several reasons justify granting privacy rights to foreign nationals. First, privacy is now a major international issue. It is common for national privacy laws in other countries to grant rights to all, regardless of citizenship. If U.S. law fails to grant rights to foreign nationals, then eventually other countries may deny rights to U.S. citizens. The issue then is as much about rights of U.S. citizens as it is about rights of foreign nationals.

Second, some other countries are already aware of the limits of the Privacy Act, and the U.S. was essentially forced to respond to the EU's unhappiness about it. The unhappiness was over more than just the Privacy Act, but adjusting the Act was something readily doable without much controversy. The result was the passage in 2016 of the Judicial Redress Act of 2015.[175] The Act created a convoluted way for the U.S. to grant rights under the Privacy Act of 1974 to citizens of designated foreign countries. The law resulted from negotiations between the U.S. and the European Union over general EU concerns about the limits of U.S. privacy law and the sweep of U.S. surveillance laws in the context of data sharing among nations for criminal and terrorism investigations. Support for the Judicial Redress Act came in part from the American business community, which feared that any new EU new privacy restrictions could interfere with international trade. Under the authority in the Judicial Redress Act, the Attorney General extended Privacy Act rights to citizens of EU member states.[176] Providing rights to citizens of some countries and not others is a policy not likely to survive for long. The change in the definition of *individual* to include foreign nationals will treat all foreign nationals in the same way and will make the Judicial Redress Act essentially irrelevant.

Third, the failure of the Privacy Act to grant rights to foreign nationals is partially ameliorated by the Freedom of Information Act. The FOIA allows *any person* to request records from a federal agency. It is common practice for immigrants who need federal records to use the FOIA to obtain copies of records pertaining to themselves.[177] The FOIA provides access to records, but it offers no mechanism

---

[175] Public Law 114-126, 130 Stat. 282 (2016), https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

[176] See Attorney General Order No. 3824-2017, Judicial Redress Act of 2015; Attorney General Designations, 82 Fed. Reg. 7860 (Jan. 23, 2017), https://www.govinfo.gov/content/pkg/FR-2017-01-23/pdf/2017-01381.pdf; Attorney General Order No. 4381–2019, Judicial Redress Act of 2015; Attorney General Designations, 84 Fed. Reg. 3493 (Feb. 12, 2019), https://www.govinfo.gov/content/pkg/FR-2019-02-12/pdf/2019-01990.pdf. See also Department of Justice, Judicial Redress Act of 2015, https://www.justice.gov/opcl/judicial-redress-act-2015.

[177] Exemptions in the FOIA and the Privacy Act are not identical so some records available under one law may be withheld under the other. A provision of the bill requires agencies to provide individuals requesting records under the USA FIPS Act with any records that would also be available under the FOIA.

that allows a data subject to seek an amendment of a record. The FOIA includes exemptions that protect national security, law enforcement, and other interests by allowing agencies to withhold records from requesters.

I note here that the FOIA has generally been held to deny use of the law to fugitives from justice.[178] That same policy applied to a revised privacy law will also ameliorate concerns about the use of the law by high-profile international criminals.

Fourth, the Privacy Act and the proposed replacement bill both contain similar exemptions that also protect national security and law enforcement interests by allowing the withholding of some records from requesters. These exemptions apply to all individuals, and both the FOIA, the Privacy Act, and the bill include complete protection for all classified information.

Fifth, until recently, the concerns that resulted in the denial of rights to foreign nationals appear to have substantially dissipated over the years. For administrative and other reasons, some agencies as a matter of discretion typically grant Privacy Act rights to foreign nationals when no reason existed not to grant those rights. Agencies cannot always tell if an individual seeking to exercise a right under the Privacy Act is a citizen. In those cases where no countervailing interest exists, it can be easier to grant rights to a requester rather than the conduct a citizenship inquiry for all requesters. For requirements of the Act that do not involve access and amendment rights, an agency may have a system of records that includes both citizens and foreign nationals. The agency must maintain the system and comply fully with those requirements for all records. Even systems that mostly have records about foreign nationals may occasionally have records about U.S. citizens. Because of that possibility, an agency will typically maintain the entire system in accordance with general Privacy Act requirements. All of these administrative circumstances make broad compliance with the Privacy Act simpler and less expensive without much regard to the citizenship status of a data subject.

A noteworthy exception to support for granting foreign nationals rights under the Privacy Act comes from President Trump. A 2017 Executive Order included this provision:

> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.[179]

---

[178] See Department of Justice, The United States Department of Justice Guide to the Freedom of Information Act (2105 edition and updated regularly online), Procedural Requirements at 19-20, https://www.justice.gov/oip/page/file/1199421/download.

[179] Exec. Order No. 13768, *Enhancing Public Safety in the Interior of the United States*, 82 Fed. Reg. 8799 (Jan. 30, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf.

The extent to which agencies complied with this presidential order is uncertain.[180] Regardless, the revised bill will grant rights to foreign nationals as a matter of statute, rights that would not be subject to change by Executive Order.[181]

2. Data Subject

(2) DATA SUBJECT. –The term "data subject" means the individual who is the principal subject of a record.

Data subject is a new term. There is a subtle distinction between *data subject* and *individual*. An individual is someone who may or may not be a data subject. To put it another way, all data subjects are individuals, but not all individuals are data subjects. Some examples will clarify.

- One of the purposes of the new bill is to permit individuals to know how agencies process personally identifiable information. Everyone is entitled to know about agency processing of PII whether or not they are actually data subjects in any given activity.

- The existing Privacy Act provision that limits collection of information about the exercise of rights guaranteed by the First Amendment uses the term *individual*. The limitation protects individuals, whether or not they become data subjects.

- An allowable disclosure for health or safety permits sharing of information if necessary to prevent or lessen a serious and imminent threat to the health or safety of any individual or the public. It does not matter whether the beneficiary of the disclosure is either the data subject of the record or any data subject at all. As with a comparable provision in HIPAA, disclosures for health or safety or allowed to assist with threats to anyone.

- In computer matching activities, due process protections protect individuals. Many individuals will be data subjects, but some will be not because they are the subject of records maintained by state or local agencies. Only subjects of federal agency records fall under the definition of *data subject*.

Data subject is a term commonly used in national privacy laws.

---

[180] In response to the Executive Order, the Department of Homeland Security announced that it would change its longstanding policy of treating all persons in the same way under the Privacy Act of 1974. The new policy now treats "all persons, regardless of immigration status, consistent with the Fair Information Practice Principles (FIPPs) and applicable law." It is not apparent that this new practice is actually different than the old practice. DHS uses a justification other than the Privacy Act to allow foreign nationals privacy rights. See Department of Homeland Security, DHS Privacy Policy Guidance Memorandum 2017-01 (webpage), https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01. The policy itself is at https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf. The DHS action is both remarkable and strong evidence of agency interest in not having to determine immigration status when providing basic rights.

[181] President Biden revoked the Trump Executive Order on January 20, 2021. See https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-the-revision-of-civil-immigration-enforcement-policies-and-priorities/.

3. Personally Identifiable Information

(3) PERSONALLY IDENTIFIABLE INFORMATION. – The term "personally identifiable information" means information about an identified or identifiable individual, including information about location, housing, education, finances, health, employment, criminal history, military service, taxation, agency program participation, Internet usage history, or any other personal activity or characteristic, and that contains any of the following data:

(A) a name;

(B) a home address, post office box, private mail box, or other physical or postal address;

(C) an e-mail address;

(D) a telephone number or the letters and numbers of a vehicle license plate;

(E) a Social Security Number; passport number; credit or debit card number; account, license, or employee number; or other identifying number assigned to an individual;

(F) date of birth;

(G) an Internet Protocol address or any comparable successor address;

(H) any other data that permits the physical or online contacting of a specific individual;

(I) a photograph, fingerprint, genetic, or other biometric identifier;

(J) information that identifies an individual's electronic device, including an international mobile equipment identity number, media access control address, contactless chip identifier, or any information that an agency Web site or online service collects online through a computer or from the individual, individual's cell phone, or other electronic device; or

(K) other information concerning an individual processed in combination with an identifier described in subparagraphs (A) through (J).

The definition of PII has several elements. The first addresses information about an identified or identifiable individual, including information about location, housing, education, finances, health, employment, criminal history, military service, taxation, program participation (e.g., participation in a government program such as Medicare), Internet usage history, or any other personal activity or characteristic. The word *including* here (and elsewhere in the bill) means *including but not limited to*. The list of activities and personal characteristics is illustrative and not exhaustive.

An individual is identified when there is enough compiled information so that it is reasonably likely that a specific individual can be associated with the information. Reasonably likely means more than 50% likelihood, but 100% certainty is not required. A name identifies an individual, although there are times when just a name without further context is not specific enough to indicate who the individual is (e.g., John Smith). An individual can be identified without a name (e.g., the adult male living at 419 Main Street, Lima, Ohio). A collection of non-personal characteristics may be enough to identify an individual (e.g., the tallest female in the 12th grade physics class at P.S. 106 in New York City).

An individual is identifiable when there is a reasonable prospect that a specific individual can be identified using the information in question. The degree of likelihood appropriate here may depend on context. An individual who lives in a small town and has an unusual surname is more likely to be identifiable than an individual who lives in New York City and has a common surname. If information can be linked to a small number of individuals but it is not certain which one, the information should be treated as identifiable if an agency uses it to make a decision about one or more of those individuals.

Whether an individual is identifiable from a set of data also can depend on who is doing the identifying. A fingerprint found at a specific location can be an identifier. To the FBI, there is a reasonable chance that a fingerprint will identify a specific individual because the FBI has biometric databases and the capability of matching a fingerprint to one of those databases. To an agency without the fingerprint-matching resources available to law enforcement, that same fingerprint may not be identifiable information. Whether a photograph is identifiable may depend on the resources used and effort made to learn whose photograph it is. A printed grocery receipt without any identifiers may be identifiable to the grocer who sold the items to a customer using a credit card or frequent shopper card.

With the much larger availability of Internet and other resources as well as the increasing capabilities of technology to connect biometric information and other data to specific individuals, the notion of identifiability is not a fixed concept. Information may become identified because an agency made an effort to connect it to a particular individual. That same information may not be PII if the agency makes no identification effort.

Another factor can be the stakes involved in identifiability. If the decision is whether to show a particular webpage to an individual, the concerns about identifiability are lower than if the decision affects an important interest or requires due process. In determining whether a collection of characteristics is identifiable, an agency should lean on the side the treating the data as identifiable. In general, facts and circumstances matter.

Fully anonymous information is not identifiable and is not PII. However, here too, the availability of other databases (whether governmental or private) and the use of technology may make it possible to reidentify data once thought to be anonymous or pseudonymous. Factors that will determine if anonymized or deidentified information is identifiable include resources and effort. Further, the capabilities of re-identifying anonymous data change over time, so anonymity cannot be treated as a designation fixed in time

Determinations about anonymity are not always simple. Consider an agency that has a database of fully anonymized information that it cannot re-identify. The agency may treat the database as anonymous and therefore not subject to the USA FIPS Act. Yet if the agency has reason to believe that a private company may have the capability to re-identify some or all of the individuals in the database, the agency cannot release the database publicly because that action would be tantamount to identifying the individuals. Withholding may also be appropriate if the agency has reason to think that the capability of re-identifying the database may arise in the near future.[182]

A database may exist in a "quantum" state of identifiability, where it is neither wholly identifiable (and therefore subject to the USA FIPS Act) nor completely anonymous (and therefore outside the Act). Individuals in the database may not be able to exercise their rights under the USA FIPS Act because the agency cannot identify which record belongs to which individual. The proper response for the

---

[182] I proposed a legislative solution for sharing deidentified data where the possibility of reidentification still exists in fact or in theory. The legislation would create a framework for contracts supporting sharing of deidentified personal information while providing protections for privacy. The contract allows a data discloser and a data recipient to define responsibilities while the legislation provides several enforcement methods, including remedies for aggrieved individuals. Robert Gellman, The Deidentification Dilemma: A Legislative and Contractual Proposal, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1277&context=iplj.

agency is to treat the database in a manner consistent with the requirements of the USA FIPS Act other than the access and amendment rights. This "quantum" status where a database at the same time is anonymous in the hands of some and identifiable in the hands of others results because different persons have different resources and capabilities. This is parallel in some ways to data being identifiable to one individual but not to another.[183] By treating databases with uncertain status as identifiable, an agency will avoid facing the problem of a USA FIPS Act A3P springing into existence one day because of a new capability or new program that makes the records identifiable.

Another element of the definition provides examples of the type of identifiers that make information into PII. The list in the statute is not exhaustive, as the last part of the definition makes clear ("other information concerning an individual processed in combination with an identifier described" in the earlier subparagraphs of the definition). Not all listed elements are, by themselves, identifiable. A data of birth is not identifiable without additional information. An Internet Protocol address may or may not be identifiable at all times. Data of any sort that allows a specific individual to be identified or contacted consistently is identifiable, even if the name of the individual is not known to anyone. A browser cookie or browser fingerprint may allow for identification of an individual in a consistent manner even if nothing else is known about that individual. If so, that cookie or fingerprint must be treated as an identifier.

4. Agency Activity Affecting Privacy

(4) AGENCY ACTIVITY AFFECTING PRIVACY. –The term "agency activity affecting privacy" means any agency function, program, or conduct that involves the processing of a record about an individual.

As discussed above, an agency activity affecting privacy (A3P) focuses broadly on the reasons that an agency processes information, rather than narrowly on the manner in which an agency files or retrieves personally identifiable information. As explained later in this report, section 5 of the bill provides additional standards and guidance about the scope of an A3P. Agencies will have considerable discretion to decide how to lump activities into A3Ps. What works at a large agency may not work for a small agency. An A3P can encompass a large number of records and functions or a small number.

The definition does not include any express notion of maintenance or ownership. Nor does the proposed definition of *record*. If the agency activity involves the processing of a record about an individual, the function is an A3P, regardless of who owns or maintains some or all of the personally identifiable information. It does not matter if a third party owns the record processed by the agency or if the data comes from a public source. An agency that regularly processes any PII regardless of source or ownership must describe that record in its A3P notice. Suppose, for example, that an agency verifies an occupational license in a public database maintained by a state. The agency record may only show verification of the license and, perhaps, the date of verification. The A3P would have to describe that the activity includes processing of occupational license data from named databases, even if the agency record was only a tick box showing the presence or absence of a license and included no details of the license (scope, expiration, etc.).

---

[183] Consider a photograph of a ten-day old baby. Years later, the mother may recognize the baby, but without more context, no one else may be able to do the same. Whether technology will change this conclusion in the future is unknown.

In another example, suppose that an agency obtains and relies on a consumer score such as a credit or other score.[184] If the agency retains a copy of the score that it uses, that information will be a record in an A3P and subject to data subject access and amendment. If the agency looks up information about a data subject in a database held by a third party and does not copy the data in a record in an A3P, that information is not subject to access and amendment rights. As will be clear later, access and amendment rights apply only to "a record processed as part of an agency activity affecting privacy." In the case of a credit score, an agency would likely and legitimately deny a request for amendment of an accurately recorded score because a score obtained from a third party is not an agency record in the hands of the third party. The data subject might pursue rights under other laws to question the credit score held by the credit bureau. If the score changed as a result, the data subject might ask the agency to reassess the data subject's status. The data subject may seek access to information that the agency maintains about how the agency used the score.

Third party information held by an agency can still be the subject of an amendment request. In response to a request from the data subject for amendment, the agency might be asked to determine if the score is relevant to the agency decision, is accurately recorded, or is current. A requester who wants to amend an agency-held score that is accurate and current for agency purposes can still file a statement of disagreement objecting to the score in some manner (e.g., the score relies on old data or on data about another individual), to its use by the agency (e.g., the score is not relevant to the agency decision), or addressing some other element of the activity involving the score (e.g., the agency uses the score in any unfair or discriminatory manner). Other administrative remedies may also be available to a disgruntled data subject.

In these examples, it is noteworthy that other laws[185] (and not the USA FIPS Act) determine what records an agency must maintain.[186] The USA FIPS Act does not direct agencies to record information (other than disclosure history) that they do not need to record to fulfill their missions. In the occupational license example, if the agency has no programmatic reason to record an expiration data, the USA FIPS Act does not require the retention of that information just because the agency saw it. However, if that data had an effect on an agency decision, 44 U.S.C. §3101[187] would presumably require recording and retention of the data as adequate and proper documentation. If a relevant agency record is not available under the access provision of the USA FIPS Act, a data subject can use the FOIA to see that record.

5. Record

---

[184] See generally, World Privacy Forum, "The Scoring of America," (2014), https://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

[185] See 44 U.S.C. §3101, https://www.law.cornell.edu/uscode/text/44/3101 ("The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.").

[186] The USA FIPS Act provides that an agency "shall process only personally identifiable information that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by law or executive order of the President." This is a different standard than the records management law in 44 U.S.C. §3101.

[187] https://www.law.cornell.edu/uscode/text/44/3101.

(5) RECORD. – The term "record" means any personally identifiable information processed by or for an agency as part of an agency activity affecting privacy.

The Privacy Act uses the term *record*. The proposed bill uses the same term with a somewhat different meaning. Much of the substance of the current term now appears in the bill as part of the definition of *personally identifiable information*. The new term means any PII *processed by or for an agency as part of an agency activity affecting privacy*. A record is PII processed for an A3P. Ownership is not part of the definition. An agency may use PII that it does not own in its activities. In fact, ownership is not an important attribute for PII anywhere in the bill, and it is rarely important in any discussion of privacy. Possession is not necessarily a required attribute either. A record is PII processed by an agency, but it also includes a record processed *for* an agency *as part of an agency activity affecting privacy*. A record may be processed for an agency by an agency contractor. PII maintained by a third party (e.g., a credit report or a public database maintained by a State) is not processed *for* an agency. That PII is maintained by someone else for their own purposes. The use of that third-party information by a federal agency does not make that third-party information in the hands of the third party subject to the USA FIPS Act. If an agency uses third party information and keeps a copy, that copy is a record as part of an A3P.

If an agency provides a record to a third party for that third party's use (e.g., reporting on the status of a loan to a credit bureau, verifying a Social Security Number for a mortgage, etc.), the third party does not become subject to the USA FIPS Act unless the third party is accomplishing an agency mission and falls under Section 14. An agency remains responsible under the USA FIPS Act and other laws for any actions that it takes based on third party or other information and for appropriately documenting those actions.

6. Use and Disclosure

(6) USE. –The term "use" means, with respect to a record, the employment, application, utilization, examination, sharing, or transfer of the record within the agency that processes the record.

(7) DISCLOSURE. –The term "disclosure" means, with respect to a record, the release, transfer, provision of access to, or divulging in any other manner of the record outside the agency that processes the record.

In modern privacy parlance, use of a record means processing that is internal to the organization that maintains the record. A disclosure occurs when a record is transferred outside the organization. The bill's definitions reflect modern usage. Current terminology in the Privacy Act is inconsistent with modern understanding. Thus, a Privacy Act *routine use* is an external disclosure, not an internal use so the term *routine use* does not appear in the USA FIPS Act. Disclosures are either *allowable disclosures* or *agency designated disclosures*. In general, the Privacy Act lightly regulates internal uses and more heavily regulates external disclosures. The bill largely follows this pattern, but there are significant changes, mostly procedural, affecting disclosures.[188]

[188] A law journal note from 2008 analyzes court cases that turn on the meaning of *disclosure*. The note proposes a specific definition for the term that seeks to resolve the problems identified. The article is interesting and insightful, but I didn't adopt the proposed definition. Just what constitutes a disclosure, especially for information already made public in some way, and whether it is a disclosure when the information is already known to the recipient can raise hard questions. Some changes proposed in other places in the USA FIPS Act resolve, at least in part, some of the identified problems. Other aspects of the problem may be less definitional and more relevant to

7. Processing

(8) PROCESSING. –The term "processing" or "processed" means, an activity with respect to a record, including the creation, collection, use, disclosure, maintenance, storage, examination, analysis, encryption, decryption, deidentification, reidentification, erasure, or destruction of the record.

Processing is a term that does not appear in the Privacy Act. In the bill, processing means any activity with respect to a record from creation to erasure to deidentification. The Privacy Act generally uses the term *maintain* (defined as "includes maintain, collect, use, or disseminate") for this activity. The new term is more specific, but the meaning of the two terms is essentially the same. The bill uses *maintain* in its ordinary meaning of *continue or support*.

8. Agency Designated Disclosures

An *agency designated disclosure* is the successor to the Privacy Act's *routine use*. Part III of this report discusses the history and general difficulties of controlling disclosures. The first part of the response to those difficulties is a new definition that calls on agencies to provide a bit more specificity when defining external disclosures. Procedural requirements for the adoption of ADDs, which are explained later, are another part of the response.

(9) AGENCY DESIGNATED DISCLOSURE. – The term "agency designated disclosure" means a disclosure by an agency of a record from an agency activity affecting privacy that is –

(A) required or specifically authorized by Federal statute or treaty;

(B) appropriate to carry out the function of the agency activity affecting privacy from which the disclosure is made and for which the record was collected; or

(C) in support of another specified Federal activity or other specified activity for which the agency can appropriately disclose a record and the disclosure is not inconsistent with the purpose for which the record was collected.

This definition establishes three categories of ADDs. All three categories have the same status and authorize an agency to disclose a record in the same way. The goal is to make each agency determine why it chose to establish an ADD and to share with the public the general reasons for the ADD. When establishing routine uses, an agency typically publishes a justification for the routine use in the original Federal Register notice. The goal here is to make agencies include the specific category of ADD as part of the description. This will assist the reader of the description of an A3P to understand the reasons for the disclosure.

The first type of ADD covers disclosures specifically authorized by Federal statute or treaty. Any disclosure required by statute or treaty can be and must be defined as an ADD. The goal is to continue the practice under the Privacy Act whereby disclosures mandated by other statutes still require a routine use in order to fulfill the notice provision of the Privacy Act. Notice also provides the public

---

damages. If an agency discloses a record to someone who already has the information, the agency's action may well violate the Act, but damages may be minimal. Jonathan C. Bond, Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century, 76 G.W. Univ. Law Rev. 1232 (2008), http://www.gwlr.org/wp-content/uploads/2012/08/76-5-Bond.pdf.

with an opportunity to comment on a proposed ADD, which could be overly broad or inconsistent with the authorizing statute or treaty.

A qualifying disclosure is one required or specifically authorized by a statute or treaty. This means that there must be some type of express language about the disclosure in the statute or treaty. For example, 42 U.S.C. § 652(k) provides:

> (1) If the Secretary [of HHS] receives a certification by a State agency in accordance with the requirements of section 654(31) of this title that an individual owes arrearages of child support in an amount exceeding $2,500, the Secretary shall transmit such certification to the Secretary of State for action (with respect to denial, revocation, or limitation of passports) pursuant to paragraph (2).[189]

Because this statute directs the Secretary of HHS to disclose specific information for a specific purpose, it qualifies as a required disclosure. Even if the statute made the disclosure discretionary, it would still meet the test for specifically authorized. A statute must make clear what information or at least what categories of information are disclosable to meet the first standard.

If a statute simply allowed the Secretary to cooperate generally with the State Department regarding passport issuance without specifically discussing record sharing, that statute would not be specific enough to meet the first standard for an agency designated disclosure. A vaguer statute requiring "cooperation" could still meet the third standard of the ADD definition, which allows disclosures in support of another specified Federal activity or other specified activity. The third standard does not require that there be any specificity in a statute regarding the elements of a disclosure or that there be any specific statutory direction at all. A statutory authorization for cooperation is enough to make the disclosure appropriate. The third standard might not be satisfied, however, if the terms of collection said that the information collected may not be used for any other purpose.

It can be challenging for an agency to identify all the potential statutory or treaty authorities that mandate disclosures. This has been an issue at times under the Privacy Act when agencies occasionally overlook disclosure obligations by not including a required routine use. Section (16)(h) of the bill provides that an agency's failure to identify a statute or treaty requiring or specifically authorizing disclosure of a record in any notice or publication under this Act shall not overcome any requirement or specific authorization to disclose the record as provided in the statute or treaty. This language makes it clear that an agency can make the required disclosure notwithstanding the failure to list the disclosure as an agency designated disclosure. Once an agency discovers the failure to list a required or specifically authorized disclosure, the agency must promptly cure the defect.

The second type of ADD is a disclosure that is "appropriate to carry out the function of the agency activity affecting privacy from which the disclosure is made and for which the record was collected." A disclosure is appropriate when it is reasonably necessary to achieve efficient and effective implementation of a required or authorized activity and does not create an undue privacy risk. This definition sidesteps the troublesome *compatibility* standard in existing law in two ways. The disclosure must be appropriate to carry out the function of the A3P and for which the record was collected. This goes a bit beyond the undefined notion of compatibility. A classic illustrative routine use allows an agency to disclose payroll information to the Treasury Department in order to allow Treasury to pay

[189] https://www.law.cornell.edu/uscode/text/42/652.

employees. This is a good example of a disclosure that is appropriate to carry out the function of a payroll A3P.

In some ways, this second type of ADD comes close to establishing a purpose test, but *purpose* is just as troublesome a concept as *compatibility*. Compatibility as a standard in the United States, at least, has a long history of use, misuse, and avoidance. I chose to leave out an express purpose test for the same reasons that I omitted a compatibility standard. Both terms come with baggage best left behind in the limited context of this class of disclosure, namely carrying out the function of the A3P. A new, albeit somewhat vague, standard ("appropriate") – a weasel word if you will – is sufficient to provide the needed flexibility and to suggest how to make a judgment.

The notion of *appropriateness* is admittedly not much more specific than the Privacy Act's existing compatibility standard. Whether a disclosure is appropriate calls for a judgment. As I concluded in the discussion in Part III of this report about the *compatibility problem*, there is no word formula that will produce the right result every time. Human judgment is essential, but the judgment should not be that difficult for most of the second class of ADDs. If a disclosure is necessary to carry out the function of an A3P, then it can clearly be defined as an ADD. If a disclosure is not absolutely necessary but would still allow an agency to carry out the function of the A3P in a more effective and efficient manner, then an ADD would still be proper. The notion of appropriateness cannot be stretched indefinitely. There will come a time when the administrative benefit of a non-consensual disclosure is so attenuated that it would not overcome the privacy interest of the data subject. Consider a disclosure to another agency provides only a minor or occasional efficiency to the disclosing agency but exposes the data subject to serious risk of loss of a right, benefit, privilege, or status that would not occur but for the disclosure or that would occur because of the ADD without proper due process procedures that would otherwise be appropriate. An ADD for that disclosure would fall on the wrong side of the appropriateness standard.

The third type of ADD is "in support of another specified Federal activity or other specified activity for which the agency can appropriately disclose a record and the disclosure is not inconsistent with the purpose for which the record was collected." This class of disclosures requires more balancing of interests and more judgment about the propriety of a disclosure. In contrast, disclosures required by statute or treaty calls for no balancing by an agency because Congress made the balance by mandating the disclosure. Disclosures related to agency function call for an easier balancing because a disclosure related to the function that the agency defined in its A3P.

When can an agency disclose a record for a specified activity of another agency or to a third party for another purpose? A key word in the definition of the third type of ADD is *specified*. The disclosure must be for a specified federal or other specified activity. An ADD is deficient if it does not state the purpose of the disclosure or identify the activity that the disclosure supports. An ADD that allows a disclosure to another agency without more detail about the specific activity being supported is deficient. On the other hand, an ADD that allows disclosure of a health record to another agency treating the individual who is the data subject of the disclosed record is sufficiently descriptive. There is no obligation to provide more detail than *health record*. So is an ADD that allows disclosure of a health record to any health care provider treating any patient, a disclosure allowed by the HIPAA health privacy rule. In many cases, a proper description of the supported activity may be short and simple.

The third type of ADD also supports disclosures outside the federal government. The disclosures might be to state or local governments or to private sector organizations. An agency making loans to individuals might decide that reporting the loans and repayment history to a credit bureau is

appropriate and not inconsistent with the purpose for which the record about the loan was collected. The propriety of a credit bureau disclosure might vary from loan program to loan program. An agency might choose not to report loans based on status (e.g., disaster loans), that are not related to the borrower's ability to repay, or that may not require repayment at all under some circumstances.

An agency would, however, be unable to justify sharing PII with a data broker building profiles on consumers or households for use in online advertising or for consumer scoring purposes. It is not appropriate for a federal agency to support those private sector activities without specific statutory direction. Further, because online advertising and consumer scoring bear no relationship to any federal activity, an ADD for those purpose would be inconsistent with the purpose of collection. These limits on disclosure for private sector data activities remain in force even if federal agencies use some private sector data services for their own activities. Only if a private company took the disclosed data and used it *exclusively* for a federal agency would disclosure be possible. Even then, the activity could only be accomplished in compliance with Section 14 extending coverage of the USA FIPS Act to contractors and others.

The definition for third class of ADDs has a second part. It requires that "the disclosure is not inconsistent with the purpose for which the record was collected." This brings back the troublesome concept of purpose and narrowly avoids the use of a compatibility test by substituting the notion of consistency. Admittedly, this is not entirely satisfactory. The goal is to establish a somewhat higher standard by which to assess disclosures that do not directly support the function of the agency that processes the PII. The problem, as already discussed, is that it is difficult, if not impossible, to define a standard to unambiguously distinguish between disclosures that should be allowed and those that should not in all the varied circumstances that arise in federal activities. Alternatives considered included a *context* standard or a *reasonable expectation* test, but neither provides any clearer direction.

As discussed in Part III of this report, the history of computer matching illustrates the problem. Should the records of one agency be used to find fraud in a wholly unrelated program, perhaps operated by a different level of government? What we learned from computer matching is that this type of disclosure had considerable policy and political support behind it. The Privacy Act of 1974, with its vague compatibility standard, was insufficient to resist the lure of computer matching for long. The USA FIPS Act will stand in a similar ambiguous position. It offers a better basis for arguing about what is appropriate, but it will not compel one result or the other all the time.

The new standard establishes a way for an agency to resist a disclosure for an unrelated activity that it does not want to make. The agency does not need to conclude that a disclosure is affirmatively consistent with the purpose of collection, only that the disclosure is *not inconsistent* with that purpose. This form of purpose test is intentionally vague. It has a bit more backbone in that it would prevent an ADD from allowing a disclosure that violates the terms of collection, but there is a deliberate degree of vagueness and a need for judgment. An agency that chooses to disclose for an unrelated activity can do so in many instances. It can also refuse to establish an ADD because a proposed disclosure is not in the public interest or in the interest of the agency, data subjects, or federal programs. An agency can determine that the risks of a disclosure (including the risks to privacy) outweigh the benefits of a proposed disclosure. A key factor here is the exercise of human judgment about what is and is not appropriate. Another factor comes from the Principle of Purpose Specification, which becomes especially relevant when an agency considers adding an ADD to an existing A3P. The notion that *information should be processed only for the purposes specified at the time of collection* is not absolute, but adding new disclosures to an existing A3P needs an especially robust justification.

The existence of an ADD does not mean that an agency must make any disclosure allowed by that ADD. Agencies need to exercise judgments at both the wholesale level (when establishing an ADD) and at the retail level (when actually disclosing a record). An agency can refuse to establish an ADD and it can refuse to make a disclosure allowed by an ADD. Section 6(h) of the proposed bill makes this explicitly clear by providing that, except as otherwise provided by law, nothing in the USA FIPS Act requires an agency to disclose a record to anyone other than the data subject or to a parent, guardian, or other person identified in section (16)(d).

Limits on disclosures via ADDs also come from a set of new procedural requirements. The bill requires that an agency go through full notice and comment rulemaking before adopting an ADD. In addition, section (6)(f) of the bill adds several noteworthy procedural requirements explained later in this report.

In some cases, a single disclosure will fall in more than one category. A disclosure may be required or specifically authorized by law and in support of an agency activity. When more than one category applies, an agency can identify the designated disclosure as meeting both criteria.

9. Agency

(10) AGENCY. –The term "agency" means an agency as defined in section 552(f) of title 5, United States Code, and the Government Accountability Office, the Library of Congress, the Administrative Office of the United States Courts, the Government Printing Office, and the Smithsonian Institution.

The definition of agency is the same as the definition in the Freedom of Information Act, with several additions. Decades ago, I advocated extending the FOIA and the Privacy Act to include the Government Accountability Office, the Library of Congress, the Administrative Office of the United States Courts, the Government Printing Office, and the Smithsonian Institution. This bill seeks to accomplish that objective. Note that federal funds make up a large part of the Smithsonian's budget. For the most part, extending privacy law to these new agencies will primarily benefit their employees of those agencies.

Existing law apparently allows each agency to determine the scope of what constitutes the agency. OMB cited legislative history from the 1974 Act to suggest that an agency within an agency was not the intention of the Congress.[190] In theory, however, offices, units, and subdivisions of an agency might be treated as separate agencies for purposes of the Privacy Act of 1974. The scope of an agency's definition of *agency* matters because of the ease with which an agency can use information within its own borders. Section (6)(a) of the USA FIPS Act continues the policy from the Privacy Act that allows use of a record by officers and employees of the agency who have a need for the record in the performance of their duties.

---

[190] The 1975 OMB Guidelines state that the question of whether an agency can exist within another agency to be "a somewhat more complex issue." Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28950 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

The intent here is to allow each agency the discretion to determine if all agency components are part of the agency. The expectation is that agencies will likely follow current practice and apply a unitary definition that includes all agency components. However, the possibility remains that there may be a reason for an agency to treat some components as separate agencies, and nothing in the USA FIPS Act prevents an agency from exercising that choice.[191]

10. Classified Information

(11) CLASSIFIED INFORMATION. – The term "classified information" means any information (1) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy; and (2) in fact properly classified pursuant to the Executive order.

The definition of classified information is identical to the definition in the Freedom of Information Act.

11. Matching Program, Recipient Agency, non-Federal Agency, Source Agency, Federal Benefit Program, and Federal Personnel

(12) MATCHING PROGRAM. – The term "matching program" –

(A) means any automated comparison or other activity that involves the disclosure of –

(i) records processed in two or more two agency activities affecting privacy or from an agency activity affecting privacy with non-Federal agency records for the purpose of –

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under Federal benefit programs, or

(ii) Federal personnel or payroll records from two or more agency activities affecting privacy or from an agency activity affecting privacy with non-Federal agency records; but

(B) does not include –

(i) matches performed to support any research, statistical, or other activity, if the results of the matching are not intended to be used and are not used to make decisions concerning the rights, benefits, privileges, or status of specific individuals or to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(ii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, 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 the person or persons;

(iii) matches of tax information pursuant to the Internal Revenue Code of 1986 or for the purpose of intercepting a tax refund due an individual under authority granted by statute;

---

[191] When Congress established the Department of Homeland Security by placing under one roof pieces of different agencies, one consequence was the internal transfer of records that previously required routine uses. That consequence had a potentially significant effect on the privacy of data subjects because it allowed easy transfer and use of records that previously required a routine use. On the other hand, because agencies find it so easy to establish broad routine uses, the actual consequence on data subjects may be mostly theoretical, although it is true that establishing a routine use at least requires publication of the routine use for public comment.

(iv) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; or

(v) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1)).

(13) RECIPIENT AGENCY. – The term "recipient agency" means any agency, or contractor thereof, receiving records processed as part of an agency activity affecting privacy of a source agency for use in a matching program.

(14) NON-FEDERAL AGENCY. – The term "non-Federal agency" means any State or local government, or agency thereof, that receives records processed as part of an agency activity affecting privacy from a source agency for use in a matching program.

(15) SOURCE AGENCY. – The term "source agency" means any (A) agency that discloses records processed as part of an agency activity affecting privacy to be used in a matching program, or (B) State or local government, or agency thereof, that discloses records to be used in a matching program.

(16) FEDERAL BENEFIT PROGRAM. – The term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash, payments, grants, loans, loan guarantees, or other forms of in-kind assistance to individuals.

(17) FEDERAL PERSONNEL. – The term personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

These terms all relevant to computer matching were added to the Privacy Act by the 1988 Computer Matching Amendments and remain largely unchanged. There are some changes to conform to the new term *processing*. The definition of *matching program* consolidates some exceptions. All IRS exceptions are now included in Paragraph (12)(b)(iii).[192]

I omitted the existing exemption for matches performed by HHS or by the IG at HHS relating to fraud, waste, and abuse. It was matching activity by the IG at HHS that started the controversy over computer matching that ultimately resulted in the Computer Matching Amendments. There is no continuing reason for an exemption for matching activities at HHS.

D. General Processing Requirements (Section 4)

[192] One existing exception in (a)(8)(b)(x) of the Privacy Act for "matches performed pursuant to section (3)(d)(4) of the Achieving a Better Life Experience Act of 2014" is impossible to evaluate. Section (3)(d)(4) does not exist. See 5 U.S.C. §552a note (references in text). In any event, that Act is part of the IRS Code, and the USA FIPS Act contains a broad exception for matching programs under the IRS Code.

Many of the provisions in section 4 of the draft come from subsection (e) of the Privacy Act of 1974. I moved these provisions to the front of the bill because they establish general standards for agency processing activities.

1. Relevant and Necessary

(a) RELEVANT AND NECESSARY. – Each agency shall process only personally identifiable information that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by law or executive order of the President.

This provision is substantially identical to paragraph (e)(1) of the Privacy Act of 1974, with only a few minor changes in wording.

2. Direct Collection

(b) DIRECT COLLECTION. – Each agency shall collect personally identifiable information to the extent practicable directly from the data subject when the personally identifiable information may result in adverse determinations about the data subject's rights, benefits, privileges, or status under Federal programs.

This provision is similar in wording and purpose to paragraph (e)(2) of the Privacy Act. It adds the word *status* to the Privacy Act's standard phrase of "rights, benefits, and privileges." Status clarifies and modestly broadens that standard phrase. It may include employment status, immigration status, health status, or other elements associated with a data subject or a data subject's PII. For example, an individual's health status may determine how a government program treats that individual, and that determination may not line up precisely with a right, benefit, or privilege.

While both existing law and the USA FIPS Act show a preference for direct collection of PII from data subjects, that preference can be overcome for reasonable cause. An individual may not be the best or most reliable source of the individual's health information. It may be entirely appropriate to look to a health record to determine with assurance a patient's diagnosis or test result. In the case of criminal investigations, the subject of the investigation may not be either a reliable or an appropriate source. Further, asking that subject for information may reveal the existence of the investigation prematurely. When considering a hiring decision or awarding a grant, an agency may properly choose to ask others to assist in the evaluation of an individual.[193] In short, the preference for direct collection will be readily overcome for some government activities. Administrative convenience of the government alone is not likely to qualify as a reasonable basis for avoiding direct collection. In addition, when considering the use of records from commercial data providers, an agency should take into account the accuracy, currency, and reliability of those records for agency's purpose.

[193] See generally, Office of Management and Budget, Privacy Act Guidelines, 40 Federal Register 28948, 28961 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

Sidebar: To the Extent Practicable and Good Faith Effort

This is one of fourteen places in the draft bill where the phrase "to the extent practicable" appears. The Privacy Act of 1974 uses the phrase "to the greatest extent practicable" in one place, and section 5 of the Public Law (establishing the Privacy Protection Study Commission) uses the phrase "to the maximum extent practicable." The two phrases "to the extent practicable" and "to the greatest extent practicable" have the same meaning. The draft drops *greatest* and *maximum* as superfluous.

Many provisions in the bill direct agencies to achieve goals and meet standards that are not ministerial. The bill's directions cannot always be accomplished without the exercise of judgment. Agencies must decide which factors are relevant to achieving the statutory goals and how to weigh the factors and the practicalities involved. These factors and practicalities may include cost; administrative efficiency; burden on individuals; risks to individuals and agency operations; accuracy of the information; ability to verify data; and others.

The repeated reliance of the phrase "to the extent practicable" is a reflection of the difficulty of establishing and meeting general privacy standards. Bright lines separating appropriate from inappropriate conduct are often impossible to establish in statutory language. These challenges are at least in part the result of a privacy law that seeks to regulate the incredibly diverse activities of more than one hundred federal agencies. A privacy law, focused on specific, narrow, and clearly-defined activities, may be able to provide better direction, but the USA FIPS Act is a general law. The problem of writing clear and precise standards for regulating broad areas of information processing is common to many privacy laws around the world.

In addition, in several places the draft calls on agencies to make a "good faith effort" to accomplish a goal. There are similarities in that both standards push agencies clearly in a specific direction but allow for other outcomes for cause. A difference between the two standards is that it will be more difficult to challenge an agency's good faith effort without actual evidence of bad faith. A challenge to the practicability standard can turn more on evidence of the degree of practicability for a given action.

3. Notice

(c) NOTICE. – Each agency shall, in writing or otherwise and in understandable language, inform each data subject whom it asks to supply personally identifiable information, at the time of collection and in a manner that allows the data subject to obtain or retain a copy, of the following:

(1) the authority for the collection;

(2) the principal purpose or purposes for which the personally identifiable information will be used;

(3) the agency designated disclosures that may be made of the personally identifiable information; and

(4) whether the data subject is required by law to supply the personally identifiable information and the consequences of not providing all or any part of the personally identifiable information.

This provision derives from paragraph (e)(3) of the Privacy Act. The USA FIPS Act proposes modest changes. It drops the requirement that the notice appear on a "form" used to collect information. Instead, the requirement is to inform a data subject at the time of collection and to allow the data subject to keep a copy of the notice. For online collection, providing the capability for the individual to read and then to print, email, or otherwise save the information will satisfy the requirement. Verbal collections raise difficulties with conveying the content of privacy notices, but verbal collection is unavoidable at times. Agencies can still find a way to provide effective notice. A summary of key information and either sending data subjects to a website for more details or offering to mail a notice should work in most or all cases. The new phrase – *understandable language* – emphasizes the goal that notices should be clear.[194]

The requirement to identify the authority for the collection is the same as existing law, but the proposed bill uses fewer words. Existing law says in a parenthetical "whether granted by statute, or by executive order of the President." I dropped this language as superfluous. An agency must still identify the statute, regulation, executive order, or other authority for collection just as it must now.

The *principal purpose* language is the same as existing law.

The requirement to identify agency-designated disclosures is comparable to the existing provision that requires disclosure of routine uses.

Finally, the existing provision requires disclosure of "the effects on him, if any, of not providing all or any part of the requested information." Another part of the same existing paragraph says that the agency must state "whether disclosure of such information is mandatory or voluntary." Together, these two requirements created much confusion, particularly over what *mandatory* and *voluntary* mean. Is disclosure mandatory if the consequence of not disclosing means that an individual will not qualify for a benefit or will go to prison? Rather than try to answer these questions, the new requirement says more clearly that the agency must tell the data subject if the disclosure is required by law and the consequences of not providing all or part of the PII requested. This language should clear up the confusion engendered by the current disclosure requirement. The words *mandatory* and *voluntary* do not appear.[195]

---

[194] The 1975 OMB Guidelines make this point. See Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28961 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

[195] 1975 OMB Guidelines make the point that it was not the intent of the existing Privacy Act notice requirement to "create a right the nonobservance of which would preclude the use of the information or void an action taken on the basis of that information." That intent remains. An aggrieved data subject might have a remedy under section 18, and a different remedy might arise under section 19. See generally, Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28961-2 (July 9, 1975),

4. Determinations

(d) DETERMINATIONS. – Each agency shall process records used by the agency in making any determination about a data subject with sufficient accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the data subject in the determination.

This paragraph derives from paragraph (e)(5) of the Privacy Act. It is identical except for the substitution of *process* for *maintain*. The four identified elements (accuracy, relevance, timeliness, and completeness) still place appropriate boundaries on federal agency processing of records containing PII.

5. Disclosure

(e) DISCLOSURE. – Prior to disclosing any personally identifiable information to any person other than an agency, unless the dissemination is made pursuant to section 552, title 5, United States Code, each agency shall make reasonable efforts to assure that the personally identifiable information is accurate, complete, timely, and relevant for agency purposes.

This paragraph derives from paragraph (e)(6) of the Privacy Act. It is substantially identical, except for minor language changes.

The standard here that the information be accurate, complete, timely, and relevant *for agency purposes*, was the topic of some discussion. I proposed changing the standard so that the disclosure would be accurate, complete, timely, and relevant *for the purpose of the disclosure*. This proposal received substantial pushback. The difficulty here relates to the type of judgment an agency must make. The argument was that an agency can assess the quality of its information for its own purposes. However, requiring the agency to make judgments about the purpose of a disclosure calls for an entirely different type of evaluation. One agency may not be able to determine whether information meets the needs of the recipient. Trying to make that type of judgment could call for an extended inquiry and potential liability by the disclosing agency. Determining the relevance of PII for use by another person (e.g., a court or a physician) is both too hard and beyond the capability of an agency. As a result, I left the standard as it is in the Privacy Act.

6. First Amendment

(f) FIRST AMENDMENT. – No agency shall process a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, or by the individual, or unless pertinent to and within the scope of an authorized law enforcement activity.

This paragraph derives from paragraph (e)(7) of the Privacy Act. It is substantially identical, except for the substitution of *process* for *maintain*. This restriction on agency activity remains one of the most important civil liberties protections in the Privacy Act and in the USA FIPS Act.

---

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

7. Legal Process

(g) Legal Process. – Each agency shall make reasonable efforts to serve notice on a data subject when any personally identifiable information about the data subject is made available to any person under compulsory legal process when the process becomes a matter of public record.

This paragraph derives from paragraph (e)(8) of the Privacy Act. It is substantially identical, except for minor language substitution.

8. Safeguards

(h) SAFEGUARDS. – Each agency shall, consistent with the requirements in subchapter II of chapter 35 of title 44, United States Code, establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any data subject.

This paragraph derives from paragraph (e)(10) of the Privacy Act. The new language is substantially the same as the existing provision. It establishes the same requirement for *appropriate administrative, technical, and physical safeguards*, a phrase later used commonly elsewhere to describe the scope of security safeguards.[196] The reference to Subchapter II of chapter 35 of title 44, United States Code makes it clear that the safeguards requirement in the USA FIPS Act is not a new or different information security standard than the one that exists in current law. Security remains an important element of fair information practices, but establishing security standards can and should be done in other legislation, regulation, and guidance.

E. Agency Activity Affecting Privacy (Section 5)

The Privacy Act of 1974 directs agencies to organize their privacy activities around the concept of a *system of records*. A system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[197] The statutory test is a factual one that turns on whether an agency actually retrieves records by individual identifier. The model for the Act was the file cabinet and computer mainframe, the technologies of the 1970s. If a file cabinet contains records that agency personnel actually retrieve by name, it is a *system of records*. But another file cabinet has identical records that no one retrieves by name, it would not be a system of records. Consider two files, one with records filed by last name in one drawer and by date in the other. Only the first is likely to be a *system of records* because it is capable of retrieval by last name. Retrieval by date does not give rise to a system of records because a date is not an individual identifier.

The USA FIPS Act proposes to replace the *system of records* concept with a functionally based concept called an *agency activity affecting privacy* (A3P). Section 5 of the USA FIPS Act describes the requirements for A3Ps.

---

[196] See, e.g., the HIPAA health privacy security standards, 45 C.F.R. §§ 164.308, .310, .313, https://www.ecfr.gov/cgi-bin/text-idx?SID=873f90deccae4cf5d2f37b090941fd2d&node=sp45.2.164.c&rgn=div6.

[197] 5 U.S.C. § 552a(a)(5).

1. Scope

(a) SCOPE. – Each agency shall determine the scope of each agency activity affecting privacy so as to reflect accurately its processing of records and to do so in a manner that supports public understanding of agency operations.

The bill gives agencies broad discretion to determine the scope of each A3P. The basic requirements are that records should be organized and described in a way that (1) accurately reflects the way that the agency processes the records, and (2) does so in a manner that supports public understanding of agency operations. Under these broad standards, agencies have considerable discretion to make choices. The old retrievability standard is irrelevant as it makes little sense for today's digital records and diversity of storage mechanisms (including cloud storage).

A large agency may decide to establish multiple A3Ps for its human resources records. Records that reflect hiring may be in one A3P; payroll records may be in another A3P; health insurance and other benefit records may be in a third A3P. The choice might reflect the way that the agency organizes its HR functions, with an A3P for each office that manages an aspect of its overall HR operations. A small agency may choose to define all its HR functions in a single A3P. Even though the goals and the contents of both agency HR operations are the same, different approaches are permissible under the Act when they make sense for the agency.

2. Guidance from OMB

(b) GUIDANCE. –The Director of the Office of Management and Budget shall issue guidance to agencies about determining the scope of an agency activity affecting privacy. The guidance shall advise agencies how to address these goals to the extent practicable:

(1) the goal of grouping activities with similar or related purposes within the same agency activity affecting privacy;

(2) the goal of grouping activities based on similar authority within the same agency activity affecting privacy;

(3) the goal of keeping records eligible for exemptions separate from non-exempt activities; and

(4) the goal of defining agency activities affecting privacy so that agency designated disclosures do not apply to records unnecessarily.

An early draft of the USA FIPS Act included goals for agencies when defining A3Ps. In the end, it seemed a better approach to define the goals but to leave it to OMB to provide guidance to agencies. The role of OMB is to provide general guidance and to try to keep the agencies properly focused, particularly with an eye on making A3Ps more understandable to the public. There are four general goals:

The first goal seeks to group together activities with similar or related purposes within the same agency activity affecting privacy. An agency program may have records organized in a variety of ways. Under the Privacy Act, some program records might be systems of record on their own and some not. Records maintained in different offices (perhaps field and headquarters) might be in different systems. The first goal suggests that agencies may treat all the records for the same program or function

("similar or related purposes") in one A3P if that structure works for the agency. It is a goal, as are all the other goals, and not a requirement.

A second goal seeks to group together activities based on similar authority within the same agency activity affecting privacy. An agency may have different statutory authorities for different parts of the same function. For example, the IRS has authority for routine tax collection activities under one or more statutes. Tax enforcement authority may derive from different statutes and may be conducted by different offices within the IRS. IRS could choose to define separate A3Ps for collection and for enforcement even though both may relate to personal income taxes.

A third goal seeks to keep records eligible for exemptions separate from non-exempt activities. The objective here is to avoid the application of exemptions to records that are not eligible for the exemptions. For example, the draft bill provides exemptions from some parts of the Act for investigatory materials compiled for the purpose of determining eligibility for employment. It might be appropriate for an agency to keep those records in a separate A3P so that the application of exemptions is simpler and easier for the public to understand. For a large agency that has a separate office conducting employment eligibility review, a separate A3P might be workable. The same approach might more troublesome for a small agency with fewer personnel.

The fourth goal seeks to define agency activities affecting privacy so that agency designated disclosures do not apply to records unnecessarily. One of the consequences of large A3Ps that have large numbers of ADDs is that it may appear to both agency personnel and to the public that all ADDs apply to all records in the A3P. Narrowing the application of ADDs to circumstances where they are necessary and not applying ADDs to records where they are unnecessary makes sense and is an important objective. For example, an agency may have an A3P for managing its employee parking permits. This function would likely need only a few ADDs. By contrast, an A3P for all HR records would likely need many ADDs because general payroll and personnel functions require the disclosure of more records for different purposes. If parking and HR records are all in the same A3P, then there will be many ADDs that seemingly apply to records and functions for which disclosures are not actually necessary. Separate A3Ps would result in more precise and limited availability of ADDs.

As may be apparent from the examples, the goals here may not all be fully attainable at the same time. One goal may suggest that a single A3P is better, while the other goal suggests that multiple A3Ps will produce more precise applicable of privacy objectives. Addressing multiple conflicting and overlapping goals is not anything new for agencies.

In the case of the fourth goal's objective in more precise application of ADDs, other methods may help just as well. An agency may define a large A3P with multiple functions managed by the same office but may provide expressly that an ADD allowing disclosure of the name of a parking permit holder to a tow truck operator applies only to records that identify the name, address, and phone number of a car owner and that other ADDs for other functions of that office apply to specific functions and records and do not apply to parking activities and records.

In resolving the different goals for the same records, one agency may reach one approach and another may choose a different approach. Agency discretion is intentionally broad, but it is not entirely

unlimited. For example, it would almost certainly be inappropriate for an agency to define all of its functions in a single A3P.[198]

3. Description of A3Ps

The Privacy Act of 1974 sets out in (e)(4) the requirements for publishing a notice about a system of records. Subsection (c) of section 5 sets out similar obligations for notices about A3Ps with some changes from existing law. The discussion below highlights noteworthy differences.

(c) DESCRIPTION. – For each agency activity affecting privacy, an agency shall prepare and maintain a description that shall include –

(1) the name of the activity, the scope of the activity, each principal substantive purpose that the activity supports, and the authority for the activity, including any related information collection requests approved under the Paperwork Reduction Act;

(2) the name of the agency component primarily responsible for the activity, the principal postal, electronic mail, and website addresses of that component, and the name of other agency components that significantly participate in the activity;

(3) the categories of data subjects about whom records are processed as part of the activity;

(4) the categories of records processed in the activity;

(5) the principal information technologies employed, including any novel or innovative applications of technology; any automated decision making; any processing of records using artificial intelligence; any algorithmic development, analysis, or application; or any similar activities with the potential to affect the rights or interests of data subjects;

(6) each agency designated disclosure applicable to records processed as part of the activity, including a good faith effort to list agency designated disclosures in the approximate order in which they are likely to be used, with the most used disclosure listed first;

(7) the categories of sources of records in the activity, including any commercial, governmental, or other sources that the agency routinely reviews, consults, or otherwise uses to carry out the activity;

(8) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records in the activity, including the name and location of records disposal schedules covering any of the records;

(9) the location of the agency website and of the agency's rules where an individual can learn how to exercise rights available under this Act;

(10) whether the activity is likely to include any records subject to an exemption in section 12 of this Act; describing the reasons exempt records may be included; and describing how the exemption affects any rights available under this Act;

(11) the date the description was most recently published or amended; and

---

[198] The original OMB Guidelines offer advice to agencies about determining the size and scope of systems of records. The guidance identifies and weighs various factors that affect an agency's determination. In broad terms, the type of balancing described by OMB is compatible with the balancing among the goals identified in the USA FIPS Act. See generally, Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28962-63 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

(12) a reference where the agency publishes any personally identifiable information processing diagram for the activity and any publicly available privacy impact assessment conducted by the agency relevant to the activity.

Paragraph (1) of subsection (c) requires, among other things, that the description include each principal substantive purpose that the A3P supports. There is no existing requirement in the Privacy Act to include a purpose description in a system of record notice, but many agencies do so today. The practice developed over time, and it is a valuable addition to the description. The same is true for a description of the authority for the activity.[199] Another new addition is any information collection requests approved under the Paperwork Reduction Act and that relate to the A3P. The objective with the PRA information is to link together for the convenience of the public some of the disparate information management requirements.

Paragraph (2) modernizes the required information that informs a member of the public how to contact the agency component responsible for the A3P. The new provision does not include the existing requirement to include the title and business address of the agency official responsible for the system of records. The notion that a single official will be responsible for an A3P may be obsolete, and in any event, it is too changeable to remain as a part of a Federal Register publication. An agency can provide additional details as it chooses on its privacy website.

Paragraphs (3) and (4) are the same as existing law with only changes in terminology.

Paragraph (5) is new. It calls for a description of information technologies employed. The purpose here is to make agencies inform the public if the agency processes records using artificial intelligence, algorithms, or similar types of information technology with the potential to affect the rights or interests of data subjects. OMB may choose to provide additional guidance here to keep current over time the types of information technology that agencies should describe here.

Paragraph (6) is comparable to the existing requirement to include each routine use. A new feature here is a good faith obligation to list each agency designated disclosure in the approximate order in which they are likely to be used, with the most used disclosure listed first. The goal is to make the A3P notice more useful to the reader. Many existing SORNs have large numbers of routine uses, some of which are rarely used. By directing agencies to list ADDs in the likely order or use, readers receive the most useful information first. Agencies need not audit or record how they employ ADDs for the purpose of ordering the list. Determining the proper order necessarily calls for a judgment by the agency. Ordinarily, an agency will not be expected to republish a notice solely to adjust the order of its ADDs, but when it has another reason to republish, it may reorder the ADDs based on more recent information. If an agency chooses to categorize ADDs in classes (e.g., one set of ADDs within the same A3P for function X and another set for function Y), the agency may order the ADDs separately as appropriate to each function. An agency may choose to have a category of rarely used ADDs at the end of its list.

---

[199] Both purpose and authority descriptions are now elements required by OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, Appendix II, Office of the Federal Register SORN Template – Full Notice (undated, "Proposed"), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a_108_12_12_16.pdf . Some agencies include all the elements set out in the Circular, and some do not.

The definition of ADD sets out three categories of ADD. The description of an ADD in the A3P notice must identify the category applicable to each ADD. This might be accomplished through a parenthetical that identifies the category. As previously discussed, more than one of the three categories may apply at the same time.

Paragraph (7) expands upon the existing requirement to describe the categories of sources of records in the system. New language makes it explicit that sources include commercial, governmental, and other sources that the agency routinely reviews, consults, or uses. It is especially important for agencies to inform the public when using commercial sources. For example, if an agency has a contract with a consumer reporting agency ("credit bureau") to use credit records, it must so state. If there is a reasonable prospect that the particular source may change but not the category of sources, the agency may choose to identify the category (e.g., "credit bureau") rather than identifying which specific credit bureau it uses. If an agency routinely uses Internet search engines to find information on individuals, it must so state. If an agency routinely seeks information from social media, the agency should identify at least the major social media used. All the information about sources will help individuals figure out how particular information about them ended up in agency records. This is especially important when the agency uses the information to make decisions about individuals. It is even more important if an agency consults but does not retain a copy of information held by a third party.

Paragraph (8) is comparable to an existing requirement, but it adds the requirement to include the name and location of relevant records disposal schedules. Agencies should have this information readily at hand, and including it in the A3P notice will be a convenience to the reader. This is another modest attempt to knit together for the public some of the information management requirements for federal agencies.

Paragraph (9) replaces the current obligation to explain agency rules for access and amendment. Rather than include substantially the same information in each notice, paragraph (9) requires that an agency provide a cite to the agency rules that explains an individual's rights.

Paragraph (10) is entirely new. The USA FIPS Act takes a new approach to exemptions. Section 12 of the Act describes the exemptions, which are generally available to agencies that maintain qualifying information. Under the Privacy Act, an agency seeking to apply most of the Act's exemptions must go through a rulemaking. The USA FIPS Act drops the separate rulemaking for exemptions. When an agency publishes a notice of an A3P, the notice itself must go through full public notice and comment. This provides the public with an opportunity to comment on the use and scope of exemptions. Paragraph (10) tells the agency to state whether the A3P is likely to include any exempt records, to describe the reasons for the exemption, and to describe how the exemption affects rights under the Act. The discussion of Section 12 below includes more about the exemptions.

Consider when an agency has a large A3P consolidating multiple functions belonging to a single office. If some of those functions may have exempt records, the description can identify those records and functions that may qualify for exempt status. Just as importantly, the description can identify those records and functions that are not likely to qualify for or need any exemption.

It would be inappropriate for an agency's notice to "claim" all theoretical exemptions for every A3P just on the off chance that one might be appropriate someday under a remote contingency. In most cases, it should not be difficult to predict whether an agency activity will include any exempt records. For many A3Ps, it will likely be clear that the activity will never have exempt records at all. For cases in

which an exempt record unexpectedly ends up as part of an agency activity affecting privacy, the failure to identify the possibility of an exemption in the description is not fatal. The agency can still claim the exemption. The agency can also cure the notice defect later if it decides that the issue is likely to recur and is not just a one-off matter.

Paragraph (11) is new. It requires that each A3P description include the date of the most recent publication or amendment. Under the Privacy Act of 1974, agencies sometimes waited years or decades before reviewing and updating systems of records. There was no simple way to find out how old a SORN was. With the new requirement, each description of an A3P will essentially tell the reader how old the description is. This may provide a clue about the currency of the description.

Paragraph (12) is also new. Section (9)(d) of the USA FIPS Act requires, to the extent practicable, the Chief Privacy Officer to maintain a personally identifiable information processing diagram or equivalent for each major A3P. Section 11 of the Act requires agencies to undertake privacy impact assessments for A3Ps. There is more discussion of the personally identifiable information processing diagram and privacy impact assessment requirements later in this document. Paragraph (12) requires that an A3P description provide a reference to any available personally identifiable information processing diagram and to any available privacy impact assessment. An agency may provide that reference at the time of publication of the A3P description. If the agency finalizes an A3P description before either document is available, it may publish a link to agency website where the documents will appear when available or when amended. An agency does not have to republish an A3P description solely to update a link to a personally identifiable information processing diagram or privacy impact assessment.

4. Publication of A3P Notices

Section (e)(4) of the Privacy Act of 1974 requires agencies to publish notices in the Federal Register when establishing or revising a system of records. Section (e)(11) requires 30 days advance notice of routine uses. The original OMB guidelines state that these publication requirements are "designed to supplant the informal rule-making provisions of 5 U.S.C. 553" but that the accommodation of the public comments in the judicial review of the rule-making exercise was intended wherever practicable."[200]

(d) PUBLICATION. – An agency shall publish the following notices, including the description of each agency activity affecting privacy prepared as provided in subsection (c) –

(1) For the initial publication of a description of an agency activity affecting privacy, the agency shall publish a complete notice in the Federal Register as provided in section 553(b) and (c) of title 5, United States Code.

(2) For any material change in an agency activity affecting privacy, including a new or modified purpose or agency designated disclosure, the agency shall –

(A) publish a notice of the proposed change in the activity in the Federal Register as provided in section 553(b) and (c) of title 5, United States Code;

---

[200] Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28966 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

(B) provide, either as part of the Federal Register notice or on the agency's website, the full text of the description of the activity clearly identifying the proposed change; and

(C) if the agency only provides the full text of the description on its website, make the full text available on or before the date when the public comment period begins.

(3) For a non-material change in an agency activity affecting privacy or in an agency designated disclosure, the agency shall publish a notice describing the change in the Federal Register and provide on its website the full text of the revised description of the agency activity affecting privacy that clearly identifies the proposed change.

The USA FIPS Act makes notice-and-comment rulemaking a requirement for initial publication of an A3P, for material changes, including new or modified purposes and ADDs. The purpose is to give the public a clearer opportunity to participate in agency decisions about A3Ps and ADDs, including the possibility of judicial review.

Paragraph (d)(2) includes a requirement that agencies publish the full text of an A3P description for any material change. For material changes, an agency has the option of publishing the full text in the Federal Register or of publishing a description of the change in the Federal Register with the full text on its website. Full notice-and-comment requirements still attach if an agency selects the website publication option.

For non-material changes, an agency must publish a summary Federal Register notice with the full text on its website. No notice-and-comment obligation attaches to non-material changes. Publication in part on an agency website may reduce the publication burden on agencies slightly.

5. Full Text Requirement

(e) FULL TEXT REQUIRED. – In any published description or proposed modification of an agency activity affecting privacy or agency designated disclosure, an agency shall include the full text of each agency activity affecting privacy or each agency designated disclosure and not by reference to another document.

Under the Privacy Act, agencies sometimes only publish the changed words of an existing SORN with little context. In order to piece together multiple changes to a SORN, a researcher may find it necessary to look through a series of Federal Register publication over many years. The USA FIPS Act expressly prohibits this practice of cut-and-paste amendments. An agency must, for all material changes, republish the full text of an A3P notice and must indicate the proposed change. The full text must appear wherever (Federal Register or website) the agency chooses to publish the text of the description as allowed by this subsection. A provision in section 16(g)(2) requires an agency to maintain a full ten-year history of all changes to each A3P description. These new requirements will enable the public to trace the history of changes more easily.

Another consequence of the full text requirement is to ban the use of generally applicable or blanket ADDs applicable automatically to all agency A3Ps. Each ADD must be adopted for each relevant agency activity affecting privacy through the notice and comment process. Blanket routine uses create confusion for both the public and for agency personnel. Often, neither is aware that blanket routine uses exist or apply. The practice of blanket routine uses sometimes results in the application of inappropriate routine uses to new systems of records. By requiring agencies to list each ADD in the

published description of an A3P, the relevance and necessity of each ADD should be reviewed and only those ADDs that are justified should be included.

6. Joint A3Ps

(f) JOINT AGENCY ACTIVITIES AFFECTING PRIVACY. – The Director of the Office of Management and Budget shall issue guidance covering any agency activity affecting privacy operated by one agency on behalf of one or more other agencies or for which more than one agency has a responsibility. The guidelines shall prescribe how the requirements of this Act shall be allocated among the agencies involved and how the duties imposed by this Act shall be carried out.

The original Privacy Act did not expressly provide for systems of records that involve more than one agency. Government-wide SORNs evolved quickly because some government records do not fit into the Act's model whereby one agency fully controls one system of records. For example, the Office of Personnel Management identifies three types of SORNs overall. The first type is *internal*, which are records owned and controlled entirely by OPM. The second type is *government-wide*, which are records for which OPM writes the policy and has some degree of control but does not have physical custody as a matter of necessity (e.g., general personnel records). The third type is *central*, which have records for which OPM writes the policy and actually has physical custody (e.g., retirement records). Federal agencies may maintain copies.[201] The OPM categories are useful, and there may be other types of joint-agency SORNs.

The Federal Privacy Council defines a government-wide system of records as "a system of records where one agency has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all of the records regardless of their custodial location."[202] The Council also maintains a list of government-wide SORNs, which the website notes may not be complete.[203] The list shows that at least ten agencies have authority over one or more government-wide SORNs.

Joint agency activities affecting privacy create issues that are hard to address in legislation. Essentially, addressing them would take many words, and there is a reasonable chance that the legislation might fail to cover all current types as well as those that may develop in the future. Subsection (f) gives OMB authority to issue guidance for any A3P operated by one agency on behalf of one or more other agencies or for which more than one agency has a responsibility. Current practice may be adequate to meet the need, but OMB has the ability to issue any guidance for government-wide-SORNs or any other aspect of the USA FIPS Act that needs attention in this context. OMB guidance can address the allocation of responsibilities among all agencies involved in a government-wide A3P, including who handles publication of notices and descriptions, and who responds to requests for access and amendment. However, OMB cannot waive or change any requirement of the USA FIPS Act for jointly maintained A3Ps.

---

[201] U.S. Office of Personnel Management, System of Records Notice (SORN) Guide (2010), https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf. This resource is more than ten years old, and it may be partially out-of-date.

[202] Federal Privacy Council, Government-wide SORNs (undated), https://www.fpc.gov/resources/SORNs/.

[203] Id. In 1995, OMB published a list of government-wide SORNs as Attachment C to OMB Memorandum 99-05, Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (Jan. 7, 1999), https://obamawhitehouse.archives.gov/omb/memoranda_m99-05-c/.

F. Allowable Uses and Disclosures (Section 6)

Section 6 provides a bit more detail about use of records and considerably more detail about disclosure of records than the current law. Section 6 corresponds to subsection (b) in the Privacy Act.

1. Use

(a) USE. – An agency may allow those officers and employees of the agency who have a need for a record from an agency activity affecting privacy to use the record in the performance of their duties. Nothing in this paragraph expands or reduces the ability of an agency to –

(1) use or withhold from use a record as otherwise provided by statute; or

(2) withhold a record used for one agency function from another agency function.

As explained above, the USA FIPS Act defines use and disclosure to conform to current terminology in the privacy world generally. Uses are internal to an agency.

The new provision for uses is similar to existing law in that both allow access to records by officers and employees of the agency maintaining the A3P who have a need for the record in the performance of their duties. The authority for uses is broad, and it is hard to assess how agencies actually implement existing authority. The Privacy Act only requires a history of disclosures and not of uses. Further, the Act does not require agencies to define and publish internal uses in contrast to the requirement for specifically identifying external disclosures (routine uses). Whether agencies treat the *need for the record in the performance of their duties* standard as a serious standard is not known. There is evidence of abuse of the standard for external disclosures (*compatible with the purpose for which [a record] was collected*), and it is likely that there is little actual enforcement of the *need for the record* standard. The Privacy Act did not provide for any agency oversight of internal uses.

The Privacy Protection Study Commission discussed this problem and proposed routine uses for both internal and external uses and disclosures.[204] That idea attracted little interest at the time or since. Defining external disclosures remains a challenging task, and adding any requirement that would oblige agencies to identify and define internal uses for all records would be even more challenging. I chose not to include that idea in the bill, despite support for it from some quarters. A requirement to define in advance all internal uses would be difficult to implement and would result in a huge list of uses. However, concerns remain that internal agency transfers of records may significantly intrude on privacy interests of data subjects.

In the end, the draft continues to leave it to agencies to control their own internal data sharing activities using their existing authority. The presence in each agency of a Chief Privacy Officer provides an opportunity for some oversight of uses. An office within an agency that does not want to share records with another office in that agency may take a dispute to the agency CPO for an independent review. This is another area where a process offers the prospect of controlling an activity for which no specific substantive standard is available. Internal rivalries may provide some unwitting privacy protections.

---

[204] Privacy Protection Study Commission, *The Privacy Act of 1974: An Assessment* 90-91 (1977) (Appendix 4), https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission.

Paragraphs (1) and (2) are new and underscore that internal limits on data sharing are appropriate. The first paragraph clarifies that the authority to allow internal uses does not expand or reduce the ability of an agency to use or withhold from use a record as otherwise provided by statute. For example, a statute may allow an agency to use a record for one function but not for another. The second clarifies that an agency may withhold a record used for one function from another agency function. In both cases, the point is that the authority in the USA FIPS Act does not affect in any way how an agency may allow or limit uses of records as provided by statute or as the agency deems proper. Some uses of records technically allowable under the general authority of subsection (a) may still be inappropriate or may violate other policy objectives. Given that many large agencies have multiple disparate functions under one roof, this clarification about an agency's ability to cabin use of some records is valuable.

Occasionally, an agency issued a routine use that authorizes an internal use, such as to the Inspector General of the agency. These routine uses are improper under the Privacy Act because they are not external disclosures. Access to records by an agency's Inspector General of a record processed by the agency is a use, not a disclosure. No routine use is appropriate under the Privacy Act, nor is an ADD proper under the USA FIPS Act. Nothing in the USA FIPS Act changes the authority of an Inspector General to access records of the agency it serves.

2. Disclosure

(b) DISCLOSURE. – No agency shall disclose any record 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 data subject, unless disclosure of the record is otherwise allowed under this section.

This language is substantially the same as existing law. Any agency seeking to disclose a record to any person outside the agency must find the authority for the disclosure somewhere in the USA FIPS Act. Even when another statute requires or authorizes a disclosure, an agency must still comply with the procedural requirement in the Act in order to justify the disclosure.

3. Agency Designated Disclosure

(c) AGENCY DESIGNATED DISCLOSURE. – An agency may disclose a record if the disclosure is for an agency designated disclosure adopted by the agency pursuant to section 5.

The language is the approximate equivalent of the *routine use* disclosure provision in the Privacy Act in subsection (b)(3).

4. Allowable Disclosures

(d) ALLOWABLE DISCLOSURES. – An agency may disclose a record if the disclosure is the following:

Existing law sets out twelve conditions of disclosure that allow an agency to disclose a record from any system of records without the need to publish a routine use. One paragraph in subsection (b) of the Privacy Act covers internal uses, which the USA FIPS Act treats in a different subsection. One of the existing paragraphs covers *routine uses*, disclosures now covered by subparagraph (c) as agency

designated disclosures. That leave ten disclosures applicable to all systems of record. Some describe these disclosures as *statutory routine uses*. The USA FIPS Act has thirteen equivalent types of disclosure authorized for all A3Ps.

It was a difficult decision to choose which disclosures to include in the statute as allowable disclosures for all A3Ps. The draft bill includes some existing disclosures as they are and modifies some others. A few are entirely new. The draft does not include some standard disclosures used in nearly all SORNs today. An example is disclosure to the Department of Justice for litigation involving agencies. In some cases, the decision to leave a disclosure off the list of allowable disclosures turned on small factors. A larger factor was the relative ease of adding ADDs to A3Ps as compared to amending the law.

a. Required by FOIA

(1) REQUIRED BY FOIA. – The disclosure is required under section 552 of title 5, United States Code.

Paragraph (1) of subsection (d) covers disclosures required under the Freedom of Information Act. This is existing law, and the result is to leave the relationship between the FOIA and the USA FIPS Act just as the relationship between the FOIA and the Privacy Act. If PII must be disclosed to a requestor (other than the data subject) under the FOIA, then disclosure under the USA FIPS Act is permissible. The public interest in balancing public and private interests in the disclosure of personally identifiable information remains unchanged.

b. Statistical Agency Disclosure

(2) STATISTICAL AGENCY DISCLOSURE. – The disclosure is to a statistical agency or unit for statistical purposes, as those terms are defined in section 3561 of title 44, United States Code, and subject to the provisions, including the limits on use and disclosure, of section 3572 of title 44, United States Code.

Paragraph (2) replaces the existing provision allowing disclosure to the Bureau of the Census. The existing provision is too narrow because there are many other statistical agencies or components with functions comparable to the Census Bureau and that have similar privacy limitations on the use and disclosure of information they obtain for statistical purposes. The draft effectively acknowledges the changes made to statistical law and policy by the Foundations for Evidence-Based Policymaking Act of 2018.[205] Existing statutory prohibitions[206] against using data collected for statistical purposes for other purposes provide sufficient protections to individuals to warrant striking the balance here in favor of allowing statistical activities that provide broad public benefits.

c. Archives Disclosure

(3) ARCHIVES DISCLOSURE. – The disclosure is to the National Archives and Records Administration –

[205] Public Law 115-435, Act of Jan. 14, 2019, 132 STAT. 5529.

[206] 44 U.S.C. § 3572, https://www.law.cornell.edu/uscode/text/44/3572.

(A) for a record that has sufficient historical or other value to warrant its continued preservation by the United States Government;

(B) for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has that value; or

(C) pursuant to a records management inspection as provided in chapter 29 of title 44, United States Code.

Paragraph (3) expands upon an existing provision that allows disclosure to the National Archives and Records Administration for assessment of historical value and for preservation. The new provision allows disclosure for the same functions. In addition, the new provision also covers disclosure for a records management inspection. The latter disclosure is a routine use found commonly in most SORNs.

d. Request from Law Enforcement Agency

(4) REQUEST FROM LAW ENFORCEMENT AGENCY. – The disclosure is to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality made a written request to the agency that processes the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

Paragraph (4) continues, almost verbatim, the existing provision that allows an agency to disclose a record to any agency of any governmental jurisdiction under the control of the United States for a civil or criminal law enforcement activity authorized by law if the head of the agency[207] makes a written request specifying the portion of the record sought and the law enforcement activity involved. The danger of indiscriminate disclosures here is reduced because a federal agency can refuse a request made in accordance with this provision, because the request must specify the particular portion of the record desired, and because the requesting agency must indicate the specific reason for the request. The requirement for a specific reason for the request and for a particular portion means that blanket requests for all information about an individual are not within the scope of this authorized disclosure.[208]

e. Civil or Criminal Law Enforcement

(5) CIVIL OR CRIMINAL LAW ENFORCEMENT. – The disclosure is to the appropriate Federal, State, local, tribal, or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the record is relevant to a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving agency.

---

[207] The 1975 OMB Guidelines approve the possibility that the authority may be delegated to lower-level officials, and that policy makes sense here (but not in other places in the bill where references to the head of the agency appear). See Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28955 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

[208] See id. at 28955.

Paragraph (5) provides for a different flavor of law enforcement disclosure. It allows a disclosure of a record to any federal, state, local, tribal, or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation or order if the record is relevant to a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving agency. This authority is new to the statute, but it reflects a routine use commonly adopted by agencies for most systems of records.

There are several major differences between the disclosure authority in paragraphs (4) and (5). Paragraph (4) requires a request from the agency that wants to use the record, and only requests from United States jurisdictions qualify. Paragraph (5) allow a disclosure with or without a request from the receiving agency, and it specifies that state, local, and foreign agencies can be recipients. I added paragraph (5) because agencies need the ability to refer matters to law enforcement on their own initiative and without waiting for a request. The breadth of the disclosure authority granted here is modestly troubling, but the need is real and a statutory solution is better than forcing agencies to adopt ADDs that might be even more open-ended.

f. Health or Safety

(6) HEALTH OR SAFETY. – The disclosure is to a person if –
(A) the agency believes in good faith that –
(i) the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any individual or the public and
(ii) the person is reasonably able to prevent or lessen the threat; and
(B) the agency making a disclosure under this paragraph sends a notice of the disclosure to the data subject's last known physical or electronic mail address, unless the Chief Privacy Officer determines that sending a notice would be inappropriate and documents the reason for the determination in writing.

Paragraph (6) expands on an existing provision that allows disclosures pursuant to a showing of compelling circumstances affecting health or safety of an individual, with notice to the individual to follow. The revised disclosure authority accomplishes the same purpose by borrowing more focused language from the HIPAA health privacy rule.[209] Paragraph (6) allows disclosures believed in good faith to be necessary to prevent serious and imminent threats to the health and safety of any individual or to the public. When making a disclosure under this authority, an agency should disclose only information necessary for addressing the threat as best as the agency can judge under what are likely to be emergency circumstances. As with the existing Privacy Act provision (and unlike the HIPAA provision), paragraph (6)(B) requires after-the-fact notice of the disclosure to the data subject of the disclosed record but allows the agency Chief Privacy Officer to forego notice if "inappropriate" and if documented in writing. Notice might be inappropriate, for example, when the data subject was the source of the threat and there is reason to believe that providing notice might place agency personnel at risk.

Each agency can decide on its own procedures for using the health or safety disclosure authority. It was tempting to assign the responsibility to the Chief Privacy Officer, but that choice might be too limiting in emergency circumstances. It might still be the right choice at some agencies, however. The

[209] 45 C.F.R. § 164.512(j).

CPO has a role to play after-the-fact if the agency does not want to send a notice of the disclosure to the data subject.

g. Congress

(7) CONGRESS. – The disclosure is to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any the joint committee.

Paragraph (7) is, except for editorial changes, same as an existing provision. It authorizes disclosure to either House of Congress or any congressional committee or subcommittee.

h. Written Inquiry to Member of Congress

(8) WRITTEN INQUIRY TO MEMBER OF CONGRESS. –The disclosure is to a Member of Congress in response to a written inquiry by the Member of Congress after the Member of Congress receives a written request from the data subject pertaining to or concerning a matter contained in the record.

Paragraph (8) addresses disclosures made at the request of an individual Member of Congress. Paragraph (8) is new. Many agencies use a routine use for these congressional disclosures, and there is some variation in the details. The purpose here is to standardize all disclosures to Members who receive requests for assistance from individuals. The provision here does not require that a data subject be a constituent of the inquiring Member. It is sufficient that a Member makes an inquiry on someone's behalf and at their request. Both the request from the data subject and the request from the Member must be in writing, and an agency should take the Member's word that there is a written request. Because a data subject's request may cover other matters or include details that are none of the agency's business, there is no requirement that the agency must see or have a copy of the written request.

i. Government Accountability Office

(9) GOVERNMENT ACCOUNTABILITY OFFICE. – The disclosure is to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.

Paragraph (9) allows disclosure to the Government Accountability Office in the same manner as existing law.

j. Contractors, Grantees, Others

(10) CONTRACTORS, GRANTEES, OTHERS. – The disclosure is to a contractor, grantee, consultant, or volunteer performing or working on a contract, grant, cooperative agreement, or otherwise for the agency and who has a need for the record in the performance of their duties for the agency. When required, the recipient shall comply with section 14.

Paragraph (10) is new and based on a routine use commonly used by most agencies for many systems of records. The new allowable disclosure permits agencies to disclose a record to contractors,

grantees, consultants, or volunteers working in some fashion for the agency and who have a need for the record in the performance of their duties. The standard is the same as the one that governs use by agency officers and employees. Section 14 of the USA FIPS Act requires agencies to apply the terms of the Act to contractors and other recipients. However, section 14 will not apply to all authorized recipients under paragraph (11). For example, a volunteer who uses agency records will not be establishing or operating an A3P for an agency in a manner that requires the agency to apply section 14.

k. Courts and Litigation

(11) COURTS AND LITIGATION. – The disclosure –

(A) is pursuant to the order of a court of competent jurisdiction;

(B) occurs in a filing made in a court of competent jurisdiction pursuant to the rules of that court;

(C) is to a party in litigation with the agency, is authorized by the rules or order of the court or adjudicative body conducting the proceeding before which the litigation is pending, and a rule, order, or a signed written agreement, limits use of the disclosed record to the purpose of conducting the litigation; or

(D)(i) is to a party, or potential party, to litigation with the agency, or to the party's authorized representative, or to an independent mediator, in connection with settlement discussions; and

(ii) the disclosure of the record is limited to the purposes of the settlement negotiations by (I) a rule or order of the court or adjudicative body conducting the proceeding, or (II) a written agreement signed by the parties.

Paragraph (11) is partly new. It covers disclosures to the courts and in connection with litigation. There are four types. The provision allows 1) disclosure of a record ordered by a court of competent jurisdiction; 2) a disclosure made in a court filing under court rules; 3) disclosure of a record to a party in litigation with an agency as authorized by court rules or a court order, if subject to a rule, order, or signed written agreement limiting use of the record use of the record to the purpose of the litigation; and 4) disclosure to a party or potential party to litigation in connection with settlement discussions and if disclosure is limited to the purpose of the settlement negotiations by court order, rule, or signed written agreement.

The first of these disclosures is existing law.[210] The current provision generated a considerable amount of litigation. Reenacting the existing provision is not intended to upset existing understandings, in particular, *Doe v. Di Genova*[211] (requiring an order specifically approved by a judge and not a court clerk).

The other three classes of disclosure are new. They reflect routine activities that occur in litigation, and all appear in routine uses adopted by many agencies. Several of these litigation-related allowable disclosures mention limits on use and disclosure. The goal here is to allow orderly disclosures that are necessary to litigation or that will aid in resolving litigation.

---

[210] 5 U.S.C. § 552a(b)(11).

[211] 779 F.2d 74 (D.C. Cir. 1985).

The appropriate use of protective orders or other approaches to control agency records shared in litigation protects data subjects against a variety of privacy harms. Those protections are welcome and encouraged. The limited mention of restrictions in these allowable disclosures reflects a reluctance to interfere unduly with processes and procedures already well-established in court rules.

I. Data Breach Response

(12) DATA BREACH RESPONSE. – The disclosure is –
(A) for the purpose of responding to a suspected or confirmed data breach that involves a risk of harm to an individual or a data system;
(B) approved by –
(i) the head of the agency;
(ii) the Chief Privacy Officer of the agency;
(iii) a senior agency official designated under a written agency data breach response plan; or
(iv) the Federal Chief Privacy Officer;
(C) of records from an agency activity affecting privacy that an agency official supervising the data breach response determines are (i) likely to be relevant to the purpose of this paragraph; and (ii) made to an agency, entity, or other person for which the official approving the disclosure has reason to believe may be able to assist in identifying the existence or scope of a data breach or in responding to the data breach either by providing a remedy for an individual who may have been affected by the data breach or by assisting with protection of a data system; and
(D) pursuant to a contract or agreement limiting the use of all data disclosed to the purpose of the disclosure and requiring either the prompt return or destruction of all data disclosed when the agency determines that the purposes of the disclosure are fulfilled.

Paragraph (12) adds a new disclosure for data breach response. The inclusion of data breach as an allowable disclosure recognizes the reality that data breaches are a standard feature of modern information technology systems.

Some existing agency routine uses for data breach date back years. Following directions from OMB, agencies more recently added routine uses for data breach response.[212] At least some agency data breach routine uses suffer from vagueness, overbreadth, or other flaws.[213] Drafting a balanced standard for data breach disclosures is a challenge because of the many ways in which data breaches can arise and in which agencies respond. The proposed statute provides for data breach disclosures as an allowable disclosure in order to establish an appropriate standard and to prevent agencies from adopting inappropriate alternatives. The allowable disclosure provides significant flexibility and relies on judgments made by agency officials with the recognition that those officials make those judgments under time pressure and in the absence of all relevant information. Data breaches typically present themselves as emergencies calling for immediate action to prevent or lessen harm.

---

[212] See Office of Management and Budget, Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[213] See, e.g., Comments of the World Privacy Forum on Department of Justice Routine Use for Data Breaches (Nov. 17, 2006), https://www.worldprivacyforum.org/2006/11/public-comments-deparpublic-comments-november-2006-privacy-act-of-1974-department-of-justice-proposes-making-changes-to-routine-uses-of-its-systems-and-databases-world-privacy-forum-files-comments-o/.

The data breach response provision has four required elements. First, the disclosure must be for the purpose of responding to a suspected or confirmed data breach that involves a risk of harm to an individual or a data system. Any risk of harm is sufficient to satisfy the standard. Any individual at risk, whether a data subject or otherwise, can qualify. The data system at risk need not be a federal agency system.

Second, a data breach disclosure must be approved by the head of the agency, or the CPO of the agency, or a senior official designated under a written agency data breach response plan, or the Federal Chief Privacy Officer. The flexibility here recognizes the need for immediate action when a breach occurs or is suspected. If a breach involves multiple agencies, the ability for the Federal CPO to authorize disclosures by more than one agency may be especially useful. The authority given to the head of the agency can be delegated to a senior agency official under the agency's data breach response plan. The necessary approval need not be in writing initially, but agencies should document approval as soon as practicable. Some existing data breach routine uses are deficient in that they either do not specify who can approve a disclosure or because they allow *any* agency employee to approve.

Third, the disclosure can include records from an A3P that an agency official supervising the response determines are likely to be relevant to the data breach response, and the disclosure is made to an agency, entity, or person that the official approving the disclosure has reason to believe may be able to assist in identifying the existence or scope of a data breach or in responding to the data breach. Legitimate goals of data breach response include providing a remedy for individuals affected by the breach and assisting with the protection of data systems. The data systems at risk do not have to be A3Ps and do not have to be federal systems at all. A data system can include a state or local government system or a private system. This provision relies heavily on the judgment of the officials involved in supervising or responding to a breach, with the full understanding that choices may need to be made in the absence of complete information about the scope or nature of a breach and that emergency circumstances may warrant decisions to be made without adequate time for full exploration of limits and alternatives. The flexibility here does not mean that officials have a blank check to disclose anything to anyone, but under all of the circumstances, officials have the ability and the responsibility to exercise judgments.

Fourth, the last requirement is that data disclosed for breach remediation be accomplished through a contract or agreement limiting use of the data to breach response and calling for the prompt return or destruction of data disclosed when the purposes of the disclosure are fulfilled. The obligation for a contract or agreement does not mandate a written document signed in advance. When an emergency does not allow time for drafting documents, oral agreements can be sufficient, and these agreements should be documented by the authorizing agency official. The provision calls for data return or destruction, but in modern information systems, neither activity may be meaningful or simple. The inclusion of a standard for promptness recognizes that immediate return or destruction may not be practical. Data may remain in backups or elsewhere in complex systems while waiting to cycle out on regular time schedules. The requirement here does not envision any extraordinary destruction measures, provided that an agency requires recipients not to process inappropriately any record awaiting destruction.

m. Federal, Personnel, and Other Decisions

(13) FEDERAL PERSONNEL AND OTHER DECISIONS. – The disclosure is to those officials and employees of a Federal agency or Federal entity that require personally identifiable information

relevant to a decision about (i) the hiring, appointment, or retention of an employee; (ii) the issuance, renewal, suspension, or revocation of a security clearance; (iii) a security or suitability investigation; (iv) the awarding of a contract or grant; or (v) the issuance of a grant or benefit.

Paragraph (13) covers several types of inter-agency disclosures relevant to personnel matters, awarding of contracts, and the like. These disclosures are common enough to warrant authorizing them as an allowable disclosure and to do so in a manner that applies the same standard to all agencies. The covered disclosures are to officials and employees of a federal agency or entity that require PII relevant to a decision about (i) the hiring, appointment, or retention of an employee; (ii) the issuance, renewal, suspension, or revocation of a security clearance; (iii) a security or suitability investigation; (iv) the awarding of a contract or grant; or (v) the issuance of a grant or benefit. The authority to disclose allows agencies to share information in order to protect legitimate governmental interests in a variety of standard activities.

One existing provision allowing disclosure does not appear in the USA FIPS Act. Section (b)(12) of the Privacy Act allows disclosure to "a consumer reporting agency in accordance with section 3711(e) of title 31, United States Code." The Debt Collection Act of 1982 added this provision to the Privacy Act of 1974.[214] Consumer reporting agencies insisted on several changes to the Privacy Act when the law authorized agencies to report federal debts to consumer reporting agencies. The changes were unnecessary. The addition of specific authority to report debts was unnecessary because each agency reporting a debt could readily add the disclosure as a routine use to the appropriate system of records. However, the argument that amendments to the Privacy Act were unnecessary did not prevail at the time. Dropping the statutory disclosure provision will require the appropriate agencies to add ADDs covering the disclosures, but the disclosures will be limited to the few A3P that need them and not to all A3Ps across government.

Nothing in the draft bill gives agencies authority to vary the terms of the allowable disclosures by issuing ADDs. There has been occasional debate over the years about an agency's authority to issue a routine use that would reduce the requirements in the statutory conditions of disclosure in subsection (b) of the Privacy Act. The intent here is that an agency may not change the provisions of any of the disclosures allowed in subsection (d) by issuing an ADD. Thus, for example, an agency cannot establish an ADD that only allows disclosure to a congressional committee when the committee affirmatively votes to ask for information. I gave consideration to adding language to expressly prohibit an agency from establishing an ADD that changes the conditions in the bill for allowable disclosures. However, in the end, the restrictive language created more problems than it solved.

5. Minimizing disclosures

(e) MINIMIZE ALLOWABLE DISCLOSURES. – When disclosing a record pursuant to an allowable disclosure in subsection (d), an agency shall make a good faith effort to disclose the minimum amount of personally identifiable information that will accomplish the purpose of the disclosure.

This provision is one of several focusing on minimizing disclosures, a goal fully consistent with the Principle of Disclosure Limitation. It directs an agency making an allowable disclosure to make a good faith effort to disclose the minimum amount of PII that will accomplish the purpose of the disclosure.

---

[214] Public Law 97-365, Act of Oct. 25, 1982, 96 Stat. 1749, https://uscode.house.gov/statutes/pl/97/365.pdf.

The basic idea is similar to the HIPAA requirement that HIPAA covered entities must make reasonable efforts to use or disclose the minimum amount of protected health information necessary to accomplish the intended purpose of the disclosure.[215] The HIPAA rule includes a number of significant exceptions that largely reflect the practicalities of health care operations.

Subsection (e) captures the flavor of the HIPAA rule with the requirement that an agency make a good faith effort to limit disclosures. It is impossible in a statute applicable to all federal agencies and programs to draw specific lines or to provide a list of exceptions. Each agency must assess the practicalities of each class of disclosure and act accordingly. For programmatic disclosures that occur routinely, an agency may determine once (perhaps with occasional reassessments) which data fields are appropriate for which disclosures. There is no need to make a choice for individual disclosures if similar disclosures can be fairly judged as a class. For one-off disclosures, however, a case-by-case assessment may be appropriate.

The HIPAA rule applies to both uses and disclosures, but subsection (e) applies only to disclosures. Subsection (4)(a) of the USA FIPS Act directs agencies to process only PII that is relevant and necessary to accomplish a legitimate purpose of the agency. That provision works to limit agency processing of PII generally. Imposing more specific limits on use – even under a good faith standard – would create unnecessary difficulties. The general limits in subsection (4)(a) serve that purpose adequately.

6. Procedural Requirements for ADDs

(f) PROCEDURAL REQUIREMENTS FOR AGENCY DESIGNATED DISCLOSURES.

Elsewhere, this report discusses the shortcomings of the *routine use* definition and its application by agencies. The discussion addresses the difficulties inherent in establishing a general standard for judging all agency defined disclosures. Subsection (6)(f) provides procedural requirements in order to make up for the inability to prescribe specific and clear substantive limitations in the definition of ADD.

a. CPO Approval

(1) CPO APPROVAL. All agency designated disclosures must be approved by the agency's Chief Privacy Officer pursuant to section 9(b)(6);

The first procedural requirement is that the agency's chief privacy office must approve each ADD. This assures that all ADDs for an agency will receive review and approval in the same manner. The CPO can refuse to allow an inappropriate, unlawful, or overly broad ADD and may restrict the terms that apply to ADD disclosures. In any bureaucratic struggle, the power to say "No" offers the CPO leverage to achieve a proper result. In the end, how agencies resolve internal disputes over ADDs is unpredictable, but the requirement for CPO approval should ensure a standard internal review. Here, as with other USA FIPS Act provisions, reliance on agency personnel to carry out their functions responsibly is essential.

---

[215] 45 C.F.R. § 164.502(b).

b. Description

(2) DESCRIPTION. – When establishing an agency designated disclosure, the agency shall to the extent practicable identify as part of the description of the disclosure –

(A) why the disclosure qualifies under one or more of the categories in the definition of "agency designated disclosure";

(B) the class of recipients of personally identifiable information;

(C) the types of personally identifiable information that may be disclosed;

(D) the purpose of and authority for the disclosure, including a good faith effort to specify each statute or treaty that requires or specifically authorizes disclosure of personally identifiable information;

(E) the position description or function of those agency officers and employees who may authorize a disclosure as an agency designated disclosure.

The second procedural requirement is the requirement to publish a full description of each ADD upon establishment. Ordinarily, this will happen when an agency establishes an A3P. The publication must explain to the extent practicable –

● Why the disclosure qualifies under one or more of the categories of ADD described in the definition of ADD. An ADD may qualify under more than one category.

● The class of recipients of PII. For example, recipients might be described as administrators of specific federal programs; health care providers treating the data subject; organizations carrying out research approved by institutional review boards; or state, local, or foreign public health departments assisting with agency public health activities and collaborative efforts. When an agency routinely shares credit information with a credit bureau, the agency may identify *credit bureaus* as the class of recipient so that the description need not change in the event that the agency uses a different credit bureau in the future.

● When an agency authorizes a disclosure to another agency, it would be appropriate to identify the part of the agency that receives the information. Thus, if would be preferable for an ADD that allows disclosure for a public health purpose to the Department of Health and Human Services to state that the recipient is the Public Health Service or the Centers for Disease Control. Still, there can be circumstances where a record has many uses within the recipient agency so that it is only practicable to identify the Department and not all the subcomponents. Similarly, when more specificity is not possible or practicable, another class of recipients might be law enforcement officials. Where description identifies a broad class of recipients, the rest of the description should provide context and place boundaries on the disclosure.

● The types of PII eligible for disclosure. There may be circumstances in which it is appropriate to disclose an entire record, but that should not be the default. A description will ideally include a list of specific categories of PII appropriate for a disclosure. If an ADD covers more than one type of disclosure, each type may have its own list of PII. For example, collaborations with public health departments may include disclosures for routine vaccinations, for contact tracing, and for pandemics. The types of PII disclosed in each case may be different, and an agency should to the extent practicable, be specific.

● The purpose of and authority for the disclosure. Some or all of the information describing purpose and authority may be covered by the description of why a disclosure qualifies under one of

the categories of ADD. An agency must make a good faith effort to specify any statute or treaty that requires or authorizes a disclosure. Another provision in the bill expressly states that failure to specify a law or treaty in an ADD does not prevent the agency from making a disclosure under the law or treaty.

● The position description or function of officers and employees who may authorize a disclosure. Many existing routine uses fail to state who in an agency can authorize a disclosure. The lack of specificity leaves open the possibility that inappropriate individuals – whether high-level political appointees or low-level employees without substantive responsibilities – can make or approve disclosures. The goal here is to describe generally the class of agency personnel who have the authority to approve disclosures. For routine and regular disclosures, it should not be difficult to describe program managers who have that authority under existing agency rules or program operations. In some cases involving non-routine matters, it may be appropriate to require approval by a designated supervisory official. For disclosures in controversial circumstances, approval by the CPO could be part of an ADD. The introductory clause – *to the extent practicable* – give agencies considerable flexibility here.

If fully complying with the description requirements for an ADD produces 25 pages of text, it would be fair for an agency to conclude that a description of that length is not practicable. There is a need to strike a balance between the length and the specificity of an ADD. An important goal is to inform the public about an agency's processing of PII. A notice that no one will read or understand fails the practicability test.

The requirements for specificity in an ADD seek to provide details that both inform the public and cabin agency choices when actually making disclosures. The use of *appropriate* as part of the statutory standard is a choice made because of the need for a degree of flexibility in giving general directions for agencies to apply in a wide variety of circumstances. However, when an agency defines an ADD, the use of *appropriate* as a descriptor is likely to be unacceptable. Thus, an ADD that allows disclosures to *appropriate* persons or in *appropriate* legal proceedings is too vague without further qualification.[216] The vagueness needed for the statute is not a model for actual ADDs. It not acceptable for the agencies to rely on vagueness when defining specific types of allowable disclosure for specific agency functions in a particular A3P.

c. Minimizing Disclosure

(3) MINIMIZING DISCLOSURE. –

(A) When establishing an agency designated disclosure, an agency shall as part of the description of the disclosure and to the extent practicable, limit each agency designated disclosure to those records and to those portions of records processed in an agency activity affecting privacy that fulfill the purpose for which the agency designated disclosure was established;

---

[216] See Department of Justice, Overview of the Privacy Act of 1974 92 (2015 edition) ("In *Krohn v. DOJ*, No. 78-1536, slip op. at 4-7 (D.D.C. Mar. 19, 1984), however, the court invalidated an FBI routine use allowing for "dissemination [of records] during appropriate legal proceedings," finding that such a routine use was impermissibly "vague" and was "capable of being construed so broadly as to encompass all legal proceedings." In response to Krohn, OMB issued guidance to agencies in which it suggested a model routine use – employing a "relevant and necessary to the litigation" standard – to permit the public filing of protected records with a court. OMB Memorandum for the Senior Agency Officials for Information Resources Management 2-4 (May 24, 1985), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/guidance1985.pdf.).

(B) When disclosing a record pursuant to an agency designated disclosure, an agency shall to the extent practicable disclose the minimum amount of personally identifiable information that will accomplish the purpose of the disclosure.

The third procedural requirement derives from language that seeks to minimize disclosures. One provision applies at the "wholesale level" when establishing an ADD. It directs an agency *to the extent practicable* when establishing an ADD to limit the scope of allowable disclosures to those records and to those portions of records that fulfill the purpose of the ADD. The second provision applies at the "retail" level when making a specific decision about the disclosure of a particular record. When actually disclosing a record under the authority of an ADD, an agency must *to the extent practicable* limit the disclosure of PII to the minimum amount that will accomplish the purpose.

For example, when an agency needs to disclose enough payroll information from a personnel record to allow another agency to pay an employee's salary, the ADD should cover only those elements needed for payroll and not the entire personnel record. For example, an earlier discussion highlighted a VA routine use that allowed the disclosure of "information" from a health record to a telephone operator facilitating phone calls for hearing impaired individuals. An ADD for that purpose should allow for the disclosure to the operator of only the information needed to facilitate the call. There is no need for an ADD to authorize the disclosure of an entire health record to the operator. However, when there are circumstances that make it impracticable to narrow down the scope of allowable disclosures in an ADD, then limits on disclosure should be applied when actually using the ADD to authorize an actual disclosure. At the "retail" level, the amount of PII disclosed may vary from case to case because the minimum necessary may be different at times.

As an example of applying the policy for minimizing disclosures, here is a revision of that VA routine use for assistance with hearing impaired calls that meets the terms of an ADD under the USA FIPS Act:

> A VA health care provider or VA administrative staff may disclose the name, phone number, and when relevant, hearing impairment of a data subject who uses telephone devices for the hearing impaired (including Telecommunications Device for the Deaf (TDD) or Text Telephones) together with the phone number and identification of the individual who will receive the phone call with the data subject, to a telephone operator or other person who facilitates phone calls for hearing impaired individuals.

In interpreting the practicability standard, an agency may be guided by established program rules or practices. If it is too difficult or cumbersome to separate out the elements of a record being disclosed, the practicability standard will allow for a broader disclosure in the ADD, leaving specific determinations to be made for each particular disclosure.

These limits on disclosure are important in part because the old notion of a system of records will be replaced by a potentially broader concept focused on functions and not records. An agency may process more PII within the same A3P so that broad disclosure authority could cover much more PII than is needed for any given disclosure. Still, the practicability standard is intended to give agencies discretion and to allow for consideration of efficiency and cost when relevant.

d. Public Disclosure

(4) PUBLIC DISCLOSURE. – If an agency designated disclosure authorizes the public disclosure of personally identifiable information, the agency shall establish a procedure that requires the approval of the Chief Privacy Officer prior to the disclosure. This paragraph does not apply to disclosures required by section 552 of title 5, United States Code, or to other public disclosures required by law.

The fourth procedural requirement provides that if an ADD authorizes public disclosure of a record or part of a record, the agency must establish a procedure that requires the approval of CPO prior to the disclosure. This limitation is a response to routine uses that allow virtually unrestricted and standardless public release of information.[217] In some instances, officials with authority to disclose information are not specified in the routine use, and the scope of the allowable disclosure can be unlimited. This type of routine use reserves too much unqualified discretion to agency officials, arguably allowing a GS-1 employee to authorize a disclosure of a record or even an entire system of records. The procedural limit comes through approval by the agency CPO. A CPO should review public disclosures under ADDs to make sure that they meet all the requirements for disclosure and that the disclosure is justified under the circumstances.

A disclosure required by the Freedom of Information Act and a public disclosure required under another statute are exempt from the requirement for CPO approval. For example, if an ethics law requires publication of information from conflict-of-interest forms, that disclosure would not require CPO approval. An agency CPO could, at the CPO's discretion, identify specific circumstances that routinely justify public disclosure of specific portions of a record and provide a specific written policy to guide public disclosures without the need for individual approval by the CPO. For example, a CPO might provide general authorization for disclosure of limited information about individuals newly appointed to senior agency positions, about arrests, or about civil or criminal court filings.

7. OMB Guidance

(g) OMB GUIDANCE. –
(1) ALTERNATIVE TO CONSENT. – The Director of the Office of Management and Budget shall issue guidance discouraging agencies from establishing agency designated disclosures principally as an alternative to obtaining consent of the data subject.
(2) MODEL NOTICES. – The Director of the Office of Management and Budget may prepare and publish for the use of agencies model notices of agency designated disclosures that are likely to be relevant to many agencies. Any agency that proposes to adopt an agency designated disclosure

---

[217] See, e.g., Drug Enforcement Administration, Training Files (JUSTICE /DEA-015) ("Release of information to the news media: Information permitted to be released to the news media and the public may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy."), https://www.govinfo.gov/content/pkg/PAI-2017-JUSTICE/xml/PAI-2017-JUSTICE.xml#dea15. This routine use suffers from many of the problems that the proposed procedural limits on ADD seek to address. The routine use does not specify what information can be disclosed, what purpose a disclosure may seek to accomplish, or which officials in the agency can release information. The vague language of the routine use ("unless it is determined") does not specify who makes the determination involved and does not explicitly require a determination by anyone prior to a disclosure. Arguably under the routine use, any disclosure authorized by the lowest level employee at whim could be justified in the absence of a determination that the disclosure would constitute an unwarranted invasion of personal privacy. In my view, this type of routine use is void for vagueness under the Privacy Act of 1974.

addressing disclosures covered by a model notice published in accordance with this paragraph that differs from the model notice by allowing for broader or additional disclosures shall explain its reasons when it publishes the agency designated disclosure for public comment.

Paragraph (g) calls on OMB to continue its traditional role under the Privacy Act of 1974 by providing guidance. The provision calls for two flavors of guidance with respect to ADDs, one required and one optional.

First, OMB must issue guidance to discourage an agency from using an ADD when it would be more appropriate to obtain consent. Relying on routine uses rather than consent is common under the Privacy Act. The practice grew up in part because agencies did not want to be bothered seeking and documenting consent. I gave consideration to banning using an ADD solely in place of consent. Instead, the bill directs OMB to issue guidance discouraging agencies from establishing agency designated disclosures principally as an alternative to obtaining consent of the data subject. This middle ground recognizes that consent may not always be practical or in the best interest of data subjects, but it seeks to establish some type of barrier to the casual adoption of an ADD in place of seeking data subject consent solely for the convenience of the agency and possibly to the detriment of data subjects.

Second, paragraph (g) allows OMB to publish model notices of ADDs likely to be relevant to many agencies. The goal is to have more uniformity when possible. OMB's discretion here is wide. For some disclosures, many agencies may have the same need to provide for a disclosure in similar circumstances. The list of allowable disclosures in Section 5 of the bill covers some but not all common disclosures. For other commonly used ADDs, OMB may offer model notices that it believes would be helpful. The bill does not require an agency to use the OMB model ADD. Instead, it provides that an agency that proposes an ADD addressing disclosures covered by an OMB model notice must explain why that ADD differs from the model if it allows for broader or additional disclosures. This is another procedural barrier against unduly expansive ADDs.

Under current practice, OMB sometimes prevents agencies from establishing a routine use that differs from one recommended by OMB. In some cases, an agency's ADD implementing an OMB model ADD may differ because it adds specificity absent from the model. That practice by itself will not trigger the need for an explanation. The concern arises if an ADD allows for broader or additional disclosures than the model OMB notice. OMB's guidance may offer further distinctions that address when an explanation is appropriate.

8. Limits

(h) LIMITS. – Except as otherwise provided by law, nothing in this Act requires an agency to disclose a record to anyone other than the data subject or to a parent, guardian, or other person identified in section 16(d).

This language makes clear that the USA FIPS Act does not require agencies to make any disclosures other than to the data subject or other person identified in section (16)(d). As with the Privacy Act, the USA FIPS Act establishes standards and procedures that an agency must satisfy before disclosing a record. Any requirement to disclose a record must derive from elsewhere. Neither the USA FIPS Act's allowable disclosures nor any ADDs adopted by an agency under its provisions mandates any

disclosures on their own. Agencies may refuse disclosures permitted by an allowable disclosure or by an ADD unless otherwise mandated by law.

G. Access to and Amendment of Records (Section 7)

1. Access

The access and amendment provisions of the Privacy Act appears to work largely as designed, and the USA FIPS Act continues the policies with several adjustments. Language that appears in section (d)(5) of the Privacy Act allowing an agency to withhold information compiled in reasonable anticipation of a civil action of proceeding no longer appears in the access section. Under the USA FIPS Act, the same authority to withhold exists, but the bill treats the authority as a formal exemption.

(a) ACCESS. – (1) An agency shall upon request by a data subject regarding a record processed as part of an agency activity affecting privacy permit the data subject and any person chosen by the data subject to review the record and to have a copy of any or all of the record in any form or format requested by the data subject if the record is readily reproducible by the agency in that form or format.

(2) An agency shall acknowledge in writing or by electronic mail receipt of a request under this subsection within ten days of receipt and shall provide the requested record within 30 days. If the request is denied in whole or in part, the agency shall inform the data subject of the denial, the reason for the denial, and the procedures established by the agency for appealing the denial to the head of the agency or designee.

(3) If after an appeal of a denial of a request for review or copy of a record, the agency refuses to provide the review or copy, the agency shall inform the data subject of the reasons for the denial and of the procedures for judicial review.

(4) For any request under this subsection and section 8(b)(2), an agency shall also provide to a data subject any requested information that would be available to the data subject under section 552 of title 5, United States Code.

Paragraph (1) of subsection (a) sets out the basic right to access of a record processed by an agency as part of an A3P. Following the lead of the Freedom of Information Act, new language directs agencies to provide a copy of a record in any form or format requested by the data subject if the record is readily reproducible by the agency in that form or format. An existing provision allowing a data subject to bring another person along to review a record remains, but language requiring a written statement authorizing discussion of the record in that person's presence no long appears because it is unnecessary. An agency can seek consent, written or otherwise for the other person under its own rules.

Paragraph (2) establishes a policy for acknowledgement of a request, a policy absent from the Privacy Act. An agency has ten days to acknowledge a request and 30 days to comply with the request. One effect of this language is to establish clearly that a requester under the USA FIPS Act has a right to administratively appeal any adverse determination of a request for access or any constructive denial following the expiration of the statutory time limit for a response.

Paragraph (3) also adds language absent from the Privacy Act requiring an agency that denies a request for access or appeal to explain the reasons and the procedures for judicial review.

Paragraph (4) is new statutory language but not new policy. It requires that an agency receiving a request for access by an individual under the USA FIPS Act must provide to the requester any information that would also be available to that requester under the FOIA. This is a long-standing policy followed by many agencies.[218] The two laws have exemptions that differ, so that information that can be withheld under one law may be disclosable under the other. The new requirement will give a data subject the most information available under either law.

Note that a provision in section 17(a)(6) addresses fees that an agency can charge for an access request.

A provision of existing law, section (f)(3), allows an agency to establish procedures for the disclosure of medical records in response to an access request. No comparable provision appears in the USA FIPS Act, with the effect that health records will be directly accessible to a requester without any limitation or procedure.[219]

2. Amendment

(b) AMENDMENT. – (1) An agency shall upon request by a data subject permit the data subject to request amendment of a record processed as part of an agency activity affecting privacy pertaining to the data subject that the data subject believes is not accurate, relevant, timely, or complete.

(2) An agency shall acknowledge in writing or by electronic mail receipt of a request under this subsection within ten days of receipt and shall within 30 days of the receipt of the request, either –

(A) make any amendment that the data subject requested, and promptly inform the data subject of the amendment; or

(B) inform the data subject of its refusal to make the requested amendment, the reason for the refusal, the procedures established by the agency for appealing the refusal to the head of the agency or designee.

(3) An agency shall within 30 days of the receipt of an appeal by the data subject of a denial of a request for amendment either –

(A) make any amendment that the data subject requested, and promptly inform the data subject of the amendment; or

(B) inform the data subject of –

(i) the right to file with the agency a concise statement setting forth the reasons for the data subject's disagreement with the refusal of the agency; and

(ii) the right to judicial review of the denial.

(4) In any future disclosure of a record or portion of a record about which a data subject filed a statement of disagreement, the agency shall clearly identify any disputed information and, unless the data subject objects in writing, provide a copy of the data subject's statement of disagreement and, if the agency chooses, a statement describing the agency's reasons for not making the amendment requested.

---

[218] See Department of Justice, Overview of the Privacy Act of 1974 119-20 (2015), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

[219] The courts largely eviscerated the existing provision anyway. See *Benavides v. Bureau of Prisons*, 995 F.2d 269 (D.C. Cir. 1993).

The amendment provision largely tracks the Privacy Act. A data subject can ask for a review of any information that the data subject thinks is not accurate, relevant, timely, or complete. This is the existing standard. The deadline for a substantive response to an amendment request is 30 days rather than "promptly" as it is in the Privacy Act. A data subject's right to file a statement of disagreement is largely the same as in the Privacy Act. An agency must mark any disputed information so that it will identify the dispute in any future use or disclosure. The statement of disagreement, together with the agency's response, must be disseminated if the agency discloses the disputed record in the future. However, the data subject may object to the dissemination of a statement of disagreement to future recipients of a disputed record. A data subject may decide that highlighting a dispute by sharing the statement of disagreement with the agency's response other will make things worse rather than better. A data subject who provides a statement of disagreement for distribution with a record cannot block dissemination of the agency's response.

3. Extension

(c) EXTENSION. – The Chief Privacy Officer may extend the deadlines for responding to a request under this section for (1) review or a copy of a record, or (2) for an amendment, in each case by no more than 30 days, by notifying the data subject making a request in writing or by electronic mail.

A 30-day extension is available for both access and amendment requests. The agency CPO may grant either or both extensions as warranted.

H. Disclosure History (Section 8)

In subsection (c), the Privacy Act requires agencies to maintain an accounting of certain disclosures. In general, disclosure histories can be useful tools that provide accountability in the processing of agency records as well as useful information to data subjects affected by agency disclosure of their records.

The terminology here has always been troublesome. The term *accounting* did not have a clear meaning to many people. Some later rules used the same term, expanding the range of confusion.[220] The USA FIPS Act seeks to address the confusion by using the more transparent term *disclosure history* rather than the existing terminology. The hope is that over time, the purpose of the requirement to keep track of disclosures will be clearer.

In my personal experience doing Privacy Act work for agencies, I found it common for agency program personnel to be unaware of the Act's requirement for disclosure accounting. At the same time, however, I also found that these same personnel invariably reported that agency operations routinely recorded disclosure histories anyway. While awareness of the Privacy Act's obligation may not have been widespread, the bureaucratic recordkeeping imperative together with other laws requiring the maintenance of records about agency activities produced the required accounting anyway. Of course, today's digital record systems often automate the maintenance of disclosure histories.

---

[220] See, e.g., the HIPAA health privacy rule, 45 C.F.R. § 164.528 (Accounting of disclosures of protected health information).

(a) ACCURATE DISCLOSURE HISTORY REQUIRED. – Each agency, with respect to each agency activity affecting privacy, shall except for uses made under section 6(a) and disclosures made under section 6(d)(1), keep or maintain the ability to create upon request an accurate history of –

(1) the date, nature, and purpose of each disclosure of a record to any person or to another agency made pursuant to an agency designated disclosure; and

(2) the name and address of the person or agency to whom the disclosure is made;

(b) RETENTION, AVAILABILITY, AND NOTICE OF DISCLOSURE HISTORY. – Each agency shall –

(1) keep or maintain the ability to create upon request a disclosure history for at least five years after the disclosure or for the life of the record, whichever is longer;

(2) except for disclosures made under section 6(d)(2), (3), (4) and (5), make the disclosure history available to the data subject upon a request made pursuant to the access procedure described in section 7(a); and

(3) inform any person or other agency about any amendment or statement of disagreement made in accordance with section 7 of any record previously disclosed to the person or agency if a disclosure history is available, if the data subject who requested the amendment or submitted a statement of disagreement asks that the amendment or statement be disclosed.

Substantively, the disclosure history provision is nearly identical to existing law. Like existing law, it covers only disclosures and not uses. It also does not apply to disclosures made in response to FOIA requests. While nothing requires agencies to maintain records of uses, agency computer systems may routinely keep those records, and usage records may be accessible to data subjects under the FOIA.

The procedure for requesting a disclosure history is the same as the access procedure set out in existing section 7(a).

Subsection (b)(2) allows agencies to withhold from a requesting data subject the history of disclosures made to statistical agencies (under section 6(d)2)); to the National Archives and Records Administration (under section 6(d)(3)); in response to requests from law enforcement agencies (under section 6(d)(4)); and for civil and criminal law enforcement (under section 6(d)(5)). Agencies must still maintain disclosure histories in these cases, but the histories may be withheld. Agencies may also choose to make these histories available in some cases as they choose. The interests being protected, be it administrative convenience or the investigative process, may not always warrant withholding. The Act's exemptions in section 12 may limit access to disclosure histories in some cases.

If an agency made an amendment or the data subject submitted a statement of disagreement, the data subject can ask that the amendment or statement (together with the agency's response) be disclosed to previous recipients. An agency should inform the data subject of these rights and of the process by which the data subject can ask for disclosure to previous recipients. A data subject can select all, some, or none of the recipients to receive the updated information.

I. Chief Privacy Officer (Section 9)

The Privacy Act of 1974 did not assign oversight responsibilities to a designated individual within each agency. As privacy legislation evolved over time and in other places around the world, the need for a privacy official to manage privacy responsibilities became a common feature. Most federal agencies have privacy offices or privacy offices, but some only have officials with little more than a privacy title.

The USA FIPS Act requires each agency to have a chief privacy officer, but nothing requires that the CPO be a full-time position. An agency's size, resources, and mission may make a difference to the amount of time that a CPO needs to perform the mission.

1. Chief Privacy Officer

(a) CHIEF PRIVACY OFFICER. – The head of each agency shall, promptly after the effective date of this Act, designate a Chief Privacy Officer to carry out the functions assigned under this Act and other related functions. If another statute established a privacy officer or similar officer for the agency, the head of the agency may designate that officer to carry out the functions assigned under this Act.

Subsection (a) requires the head of each agency to "promptly" designate a CPO to carry out the function assigned under the USA FIPS Act and "other related functions." The *other functions* language is deliberately vague. Depending on the role of the agency, there may be other privacy activities that a CPO can undertake beyond the scope of the USA FIPS Act. Much will depend on the organization of the agency, the allocation of current responsibilities, and choices made by agency management. A CPO can have expanded privacy functions when appropriate to the duties of the agency.

At a few agencies, political appointees are CPOs. The Act does not require or prevent a CPO from being a political appointee. At most agencies, however, the position is likely to be filled with a civil servant.

Some debate surrounded the time for the initial appointment of the CPO. For agencies that face long and complicated transitions from the Privacy Act to the USA FIPS Act, delay in appointing a CPO will make it difficult to complete the work required despite the generous deadlines for compliance. I considered requiring appointment of the CPO within a fixed period after the date of enactment. However, statutory deadlines of that type are often not met, and without a significant penalty, that remains a possibility. In the end, it seemed better to ask for good management than to try to mandate it. Thus, the bill calls for the prompt appointment of the CPO.

For agencies that have CPOs or similar officials either under other laws or by management designation, the head of those agencies can designate those officials to serve as the CPO for USA FIPS Act purposes.

2. Duties

(b) DUTIES. – The Chief Privacy Officer for an agency shall –
(1) have agency-wide responsibility for privacy and for compliance with fair information practices;
(2) have agency-wide responsibility for overseeing agency compliance with Federal laws, regulations, and policies relating to privacy, including primary responsibility for implementation of this Act;
(3) participate in identifying and addressing privacy risks throughout the agency;
(4) have responsibility for agency privacy impact assessments as provided in section 11;
(5) have a central role in the agency's development and evaluation of legislative, regulatory, and other policy proposals relating to or affecting the privacy of personally identifiable information; and

(6) approve the publication of the description of each agency activity affecting privacy, including each agency designated disclosure, prior to publication for comment and before the description and the agency designated disclosure becomes final.

Subsection (b) sets out a number of general duties for the CPO, and other parts of the Act give the CPO other specific functions. There should be no particular distinction between CPO functions identified here or elsewhere in the bill. The location of a function is a consequence of the drafting process and not a substantive judgment on the importance of the function.

The first of the general duties assigns the CPO agency-wide responsibility for privacy and compliance with fair information practices. Privacy management can come in many different flavors within an agency, and the other officials may have responsibilities in specific areas. It will be up to each agency to determine how to allocate privacy responsibilities among the agency's officials and programs. The Act gives the CPO a voice and a central role in privacy matters throughout the agency. The CPO's responsibility for compliance with FIPs underscores the importance of FIPs as a general goal for privacy.[221] Implementing FIPs in agency programs requires judgment because the general policies reflected in FIPs do not dictate how to apply each practice.

The second general duty for a CPO is agency-wide responsibility for overseeing compliance with all laws, regulations, and policies relating to privacy, including primary responsibility for implementation of the USA FIPS Act. Again, this gives the CPO a role in all agency matters relating to privacy. Responsibility for some privacy activities may be elsewhere in the agency as provided in other laws and as each agency sees fit to assign those responsibilities. The CPO has a voice in all privacy matters, but the CPO is primarily responsible for implementation of the USA FIPS Act. That responsibility cannot be moved elsewhere.

The third general duty for a CPO is identifying and addressing privacy risks throughout the agency. Both agencies and data subjects face privacy risks when agencies process PII. The responsibility with respect to privacy risks gives the CPO broader authority to consider how agency components address those risks. Assessing risk is important because scarce resources will be best used to address riskier activities.

The fourth general duty for a CPO is responsibility for an agency's privacy impact assessments. Section 11 of the bill provides more details about PIAs, but the point here is that the CPO manages the PIA process. Program officials also play a significant role in PIAs for their own operations, but they must work with the CPO to meet the requirements.

The fifth general duty gives the CPO a central role in the agency's development and evaluation of legislative, regulatory, and other policy proposals about privacy. This gives the CPO a seat at the table when an agency develops or evaluates matters that affect privacy, including when Congress or OMB seeks an agency's views on legislation.

The sixth general duty requires the CPO to approve the description of each A3P disclosure (and each ADD) prior to its publication for comment and before it becomes final. The emphasis on agency

---

[221] See 6 U.S.C. § 142(a)(2) (assigning the DHS privacy officer with responsibility for "assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."), http://www.law.cornell.edu/uscode/text/6/142.

designated disclosures underscores the importance of controlling and limiting ADDs. A CPO will have considerable ability to stop activities that do not comply with the Act's overall standards. When disputes arise between an agency's CPO and program officials, it will be up to each agency to find a resolution. It is not anticipated that a CPO can singlehandedly stop an activity that an agency committed to undertake, but the CPO will have a voice if privacy matters are ignored or inadequately addressed.

3. Notices

(c) NOTICES. –The Chief Privacy Officer shall, to the extent practicable, standardize elements and terminology of notices of agency activities affecting privacy, including agency designated disclosures.

Subsection (c) directs the CPO to standardize the language of A3P notices and ADDs. For example, it is not uncommon to find modest or even significant differences in routine uses that seek to accomplish the same goal within the same agency. This subsection establishes standardization as a soft goal ("to the extent practicable").

4. Personally Identifiable Information Processing Diagram

(d) Personally Identifiable Information Processing Diagram. – The Chief Privacy Officer shall, to the extent practicable, maintain on the agency privacy website for each major agency activity affecting privacy a current personally identifiable information processing diagram or equivalent document that visually depicts the collection, use, and disclosure of personally identifiable information and that shows the principal sources of information, the principal internal users of the personally identifiable information, the principal purposes for which the agency collects and discloses personally identifiable information, and the recipients of significant disclosures.

Subsection (d) establishes another soft goal ("to the extent practicable") for a CPO. A personally identifiable information processing diagram or similar document can be useful in describing the processing of PII within agency operations. Agencies may already prepare diagrams as part of system designs or for other purposes, and the some of those diagrams can and should be made available to the public when possible. While diagrams may serve other purposes in other contexts, the goal here is to provide the public with a visual description of the processing (collection, use, disclosure, etc.) of PII in the context of an A3P. Some complex A3Ps with multiple functions and data flows may require multiple diagrams.

An earlier draft of the bill made a *data map* part of each A3P. I dropped the term *data map* because it has a technical meaning in some contexts that was inappropriate here. The term *personally identifiable information processing diagram* is new, and this allows agencies (with OMB guidance) to devise a visual depiction of PII processing suitable for their own A3Ps and their own circumstances.

Not every A3P requires a visual diagram, and there may not be sufficient resources to maintain a current one at all times for every A3P. The CPO has considerable authority within available resources to determine priorities. Rather than include diagrams in Federal Register notices, the bill directs a CPO to maintain the diagrams on the agency's privacy website. This will make it easier to change the diagrams as needed. Nothing stops a CPO from publishing a diagram as part of a notice for an A3P if the CPO thinks that it would be useful to the public or to the agency.

The disclosures made of PII from an activity are an important part of any diagram. The bill calls for including *significant* disclosures because it may be impractical to include every possible disclosure. Significant disclosures are those that are a standard for an A3P's basic functions. There may be no need, for example, to include the possibility of disclosures for historical archiving purposes. However, any disclosure that has more than a minimal potential to affect a data subject should be included.

5. Report

(e) REPORT. –When the Chief Privacy Officer of an agency determines that a threat or vulnerability is creating or is likely to create a significant disruption to the privacy responsibilities of the agency, a serious unresolved privacy or security risk to the agency, or an inappropriate or avoidable serious privacy or security risk to data subjects, the Chief Privacy Officer may –

(1) consult with the Chief Information Officer of the agency; and

(2) report from time to time directly to the head of the agency.

Ideally, each agency will integrate privacy management with other information management functions. It is hard, however, to legislate good management, and information management structures vary considerably among agencies. Subsection (e) is a *break the glass* type of activity that a CPO can use when routine management reporting is not sufficient. When the CPO sees the possibility of a significant disruption to an agency's privacy responsibilities, a serious unresolved privacy or security risk to the agency, or an inappropriate or avoidable serious risk to data subjects, the CPO can take an action outside of routine channels. The provision gives each CPO the ability to report on occasion directly to the head of an agency. The standards here are relatively high. Depending on the size and functions of an agency, a CPO may be located in many different places in an agency's organization chart. The reporting option allows the CPO to bring a matter directly to the head of the agency regardless of the CPO's location within the agency. The bill also allows a CPO to consult with the agency's Chief Information Officer. This type of consultation is likely to be more routine, and a CPO may find that a visit to the CIO is a good idea prior to asking for access to the agency head.

6. Guidance

(f) GUIDANCE. –The Director of the Office of Management and Budget may issue guidance on the activities and functions of a Chief Privacy Officer, including guidance on the preparation and format of personally identifiable information processing diagrams prepared under subsection (d).

Subsection (f) allows OMB to issue guidance on the activities and functions of a CPO. OMB may also offer guidance on the preparation and format of personally identifiable information processing diagrams, with a goal of standardizing the diagrams when appropriate.

J. Federal Chief Privacy Officer at the Office of Management and Budget (Section 10)

The Privacy Act gave OMB a principal role in guiding agency compliance with the Act. Over the years, OMB's work on privacy guidance has been variable. The original OMB guidelines from 1975 were generally well done and offered agencies needed direction when the Privacy Act was new. Since that original effort, some OMB staffers responsible for the Privacy Act did an outstanding job given the constraints under which they worked. Still, OMB privacy efforts waxed and waned. Congressional and

GAO report cited earlier make the point that OMB did not always do a good job and that OMB never provided some guidance promised years ago. For brief times during the Clinton and Obama administrations, OMB created a formal privacy officer with a role that included the Privacy Act as well as other privacy matters. Neither position lasted long.

Notwithstanding OMB's inconsistent record, the USA FIPS Act still assigns a major role to OMB, largely for lack of a viable alternative. If the United States had a privacy agency – something found in just about every other country with a data protection law – that agency could be given a role under the USA FIPS Act. Creating that agency would be too difficult and too distracting to do in this proposal. The hope is that a new law combined with today's stronger political and popular interest in privacy will result in a more consistent effort from OMB.

(a) FEDERAL CHIEF PRIVACY OFFICER. –The Director of the Office of Management and Budget shall, promptly after the effective date of this Act, establish an Office of the Federal Chief Privacy Officer as part of the Office of Information and Regulatory Affairs. A Federal Chief Privacy Officer shall head the Office of the Federal Chief Privacy Officer.

(b) DUTIES. –The Office of the Federal Chief Privacy Officer shall –
(1) have responsibility for preparing Office of Management Budget guidance under this Act;
(2) provide notice and opportunity for public comment for the guidance;
(3) assist and direct agencies with the transition from compliance with the Privacy Act of 1974 to compliance with this Act;
(4) oversee agency compliance with this Act and provide continuing assistance to agencies with the implementation of this Act; and
(5) have responsibility for advising the Director on all privacy matters.

Subsection (a) requires the Director of OMB to establish an office of the Federal Chief Privacy Officer in the Office of Information and Regulatory Affairs. OIRA is the office that oversees Privacy Act activity at the agencies. I considered assigning the Federal CPO to also serve as OMB's internal CPO, but others thought that the functions should be separated. However, the bill does not prohibit the Federal CPO from serving as the internal OMB CPO.

Subsection (b) assigns the Federal CPO five main duties, mostly relating to the USA FIPS Act. In numerous places, the Act requires or authorizes OMB to issue guidance. Developing that guidance will take considerable efforts in the first few years under the Act. The second duty is providing for notice and public comment for that guidance. The goal here is to make sure that the public has an opportunity to play a role in shaping OMB guidance. The requirement is to seek public comment, but the provision does not direct OMB to undertake formal APA notice-and comment rulemaking. The third duty is to assist and direct agencies with the transition from the Privacy Act of 1974 to the USA FIPS Act. The transition will be a complex undertaking for many agencies, and OMB can do much to help. The fourth duty is to oversee agency compliance with this Act and provide continuing assistance to agencies. This is comparable to the requirement in subsection (v)(2) of the Privacy Act. The duty to *oversee* and *assist* is suitably vague, as OMB has many ways to convince agencies to comply with OMB advice. There is no need here to assign OMB specific additional power.

The final duty is advising the Director of OMB on all privacy matters. Privacy is a major subject of policy and legislative interest, and OMB may choose to give the Federal CPO other privacy responsibilities. Alternatively, a White House may decide that privacy policy matters require attention at a higher level. If so, the Federal CPO's role may remain limited to the specific statutory functions. If

not, the broad authority to advise the Director on all privacy matters may expand in privacy areas unrelated to the Act itself. The Federal Chief Privacy Officer will not be the equivalent of a data protection authority established under privacy laws of the European Union and many other countries. Most notably, the Federal CPO will not have the independence that is a hallmark of data protection authorities.

K. Privacy Impact Assessment Process (Section 11)

The Privacy Act of 1974 did not include any requirement for a privacy impact assessment. The Act predated the concept of a PIA. Yet the origin of the PIA has a Privacy Act connection. Robert N. Veeder, who served as the principal Privacy Act expert in the Office of Management and Budget during the 1980s, implemented the first PIA policy when he headed the privacy office at the Internal Revenue Service in 1996.[222] The idea of a PIA caught on much more broadly, and it is now a feature of many national privacy laws. Eventually, the Electronic Government Act of 2002 picked up on the idea and included a PIA requirement for federal agencies generally.[223] The problem with that requirement is that the mandated content of a PIA provides little more information that the Privacy Act requires in a system of records notice.[224] At some agencies, completing a PIA was a minor task, often completed in a single page, that did not contribute in any real way to the evaluation of the privacy consequences of an agency activity. OMB provided guidance[225] that improved on the limited requirements in the statute, and some agencies did a better job conducting effective PIAs.[226]

In developing the PIA provision for the USA FIPS Act, I gave consideration to including specific mandates for the content and methodology for PIAs. One point that developed from discussions was the importance of the PIA *process* as opposed to a PIA *product*. That is why the draft bill consistently refers to the PIA process. Another result is a bill that provides more guidance and gives considerable discretion to the agency CPO to adjust the PIA process to meet the agency's needs, budget, and schedule.

Another point that emerged from discussions is the difficulty of conducting PIA processes for the many different type of federal agency activities. Some activities are relatively minor in scope and consequence, while others are large and have significant privacy effects. Many activities are ongoing and have been in place for years or decades. Other new activities may arise with urgent mandates for immediate implementation. These observations also supported dropping fixed mandates in place of broad guidance and agency discretion. Not every activity needs the same type of PIA. Resources to conduct PIAs may be limited.

---

[222] In the introductory chapter to their book Privacy Impact Assessment (2012), David Wright and Paul De Hert include a table of milestones in the development of PIA methodologies. The first item in that table is the IRS PIA policy. David Wright & Paul De Hert, Introduction to Privacy Impact Assessment, Table 1.1.

[223] 44 U.S.C. § 3501 note (section 208).

[224] 5 U.S.C. § 552a(e)(4).

[225] Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (2003) (M-03-22), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22.

[226] For example, the Department of Homeland Security has a noteworthy, if inconsistent, history of conducting useful PIAs. See 6 U.S.C. § 142(a)(4).

Frankly, agencies often find ways to evade statutory mandates. In the Computer Matching Act, the law directed agencies to "assess the costs and benefits" of matching programs.[227] However, some agencies simply ignored the requirement. Other agencies provided one-line assessments, stating only that it was more cost-effective to match records by computer than by hand. OMB never issued promised standards for cost-benefit analyses. The statutory requirement faded into meaninglessness as a result of OMB indifference, the inability of congressional committees to find a way to object, and the absence of an effective way for the public to object or to litigate. Putting too much detail in a law runs the risk that agencies will find a way to evade the obligations, especially if requirements are not properly tuned to the need.

1. Purpose

(a) PURPOSE. – The purposes of the privacy impact assessment process are –

(1) to inform agency decisions for the life cycle of agency activities affecting privacy, including planning, design, implementation, and conduct, in a manner consistent with other Federal information resources management policies, principles, standards, and guidelines;

(2) to identify significant risks to the agency and significant consequences for the privacy of data subjects from the conduct of agency activities affecting privacy;

(3) to seek and implement ways to minimize significant risks and consequences prior to establishing or modifying an agency activity affecting privacy while providing for the efficient and effective conduct of agency responsibilities;

(4) to provide that agency processing of personally identifiable information minimizes the processing of personally identifiable information, maximizes fairness, includes appropriate due process protections, and generally complies with fair information practices;

(5) to provide to the extent practicable an opportunity for public comment in the planning and design of an agency activity affecting privacy;

(6) to complete the process, to the extent practicable, before the agency makes final decisions about the design of an agency activity affecting privacy; and

(7) to document the conduct of the process with a written report.

Subsection (a) identifies seven major purposes for the PIA process. The first paragraph highlights that the PIA process should inform agency decisions for the life cycle of each A3P. The PIA process is not intended as an academic exercise to be completed independently of the development of an A3P. Nor is it meant to be a compliance exercise that can be satisfied by an after-the-fact document merely justifying final programmatic and technological decisions. The PIA process should be part of the planning, design, implementation, and conduct of an A3P. The PIA process may result in appropriate change in that planning, design, implementation, and conduct, along with other factors that influence agency activities.

The second paragraph focuses on the importance of identifying significant risks to the agency and significant consequence to data subjects. These can be different risks that require different responses. For example, the collection of PII presents a risk to the agency in that it must secure the data, manage its use and disclosure, and be prepared to respond in case of data breach. The agency processing of PII can have consequences to the data subject that may include the intended use of the data, secondary uses and disclosures unrelated to the original purpose, and the effects of data breach.

---

[227] 5 U.S.C. § 552a(u)(3)(B).

The third paragraph emphasizes the importance of minimizing the risks and consequences of agency activities *prior to* starting or changing an A3P. One obvious way to accomplish both of these objectives is to collect and maintain less information. That is, of course, not always possible, and the provision recognizes the importance of efficient and effective conduct of agency responsibilities. There are always tradeoffs between major objectives. Privacy protection may rarely be the most important objective of any given program, but it will often be a relevant objective that deserves attention and weight. The need to find and minimize risks and consequences before an agency makes decisions underscores the first purpose.

The fourth paragraph identifies the goals of minimizing processing of PII, maximizing fairness, providing due process protections, and complying with FIPs.

The fifth paragraph emphasizes the importance of public comments in the planning and design of agency A3Ps. The Act provides a role for the public in the PIA process, but much will be within the discretion of agencies to decide how to bring the public into the process in a timely way.

The sixth paragraph tells agencies that they should, to the extent practicable, complete the PIA process before making final decisions about the design of an A3P. This emphasizes that the PIA process should not be a paper exercise completed after an activity starts functioning. The PIA process should influence agency design decisions and not just ratify them after the decisions are made.

The seventh paragraph makes it clear that a written report on the PIA process is another objective. The PIA report should, to the extent possible, be a document available for public review. If parts of a PIA report are classified or qualify for withholding for other reasons, then unrestricted parts of the report should still be made public.

2. Process

(b) PROCESS. –

(1) Each agency shall conduct either a thorough or a limited privacy impact assessment process for new or significantly modified agency activities affecting privacy and for new or significantly revised matching programs.

(2) In determining whether to conduct a thorough or a limited privacy impact assessment process, an agency shall consider using a thorough assessment when agency activities affecting privacy are reasonably likely to have one or more of these characteristics:

(A) affect a large number of data subjects;

(B) involve determinations of eligibility for rights, benefits, privileges, or status;

(C) employ or propose to any novel or innovative applications of technology;

(D) present significant risks to the agency or significant consequences for the privacy of data subjects;

(E) involve the routine collection of a records from sources outside the Federal government or the disclosure of large number of records outside the agency; or

(F) result in significant new mergers of previously separate government databases.

(3) The Director of the Office of Management and Budget shall issue guidance to help agencies –

(A) decide whether to conduct either a thorough or a limited privacy impact assessment process;

(B) establish priorities for conducting privacy impact assessment processes;

(C) address privacy –
(i) as part of the information and information system life cycles;
(ii) in relation to other requirements pertaining to the collection of information; and
(iii) with regard to information system development, security, and the use of information technology resources;
(D) determine when and how to conduct public consultations;
(E) conduct a privacy impact assessment process for an agency activity affecting privacy that involves more than one agency; and
(F) conduct any other aspect of the privacy impact assessment process.

Subsection (b) describes the process for agencies to follow. For new or significantly modified A3Ps or computer matching programs, there are two types of PIA processes, thorough and limited. The bill lists six factors to consider when deciding if a thorough PIA process is appropriate. The factors are whether an A3P is reasonably likely to: (A) affect a large number of data subjects; (B) involve determinations of eligibility for rights, benefits, privileges, or status; (C) employ or propose to employ any novel or innovative applications of technology; (D) present significant risks to agencies or significant consequences for the privacy of data subjects; (E) involve the routine collection of records from sources outside the Federal government or the routine disclosure of records outside the Federal government; and (F) result in significant new mergers of previously separate government databases.

The choice about a thorough or limited PIA process is ultimately up to the CPO, as provided later in this section of the bill. The presence of any listed factor does not automatically mean that a through PIA process is appropriate. Not every PIA process can or should be thorough. The choice ultimately depends in part on resources and on the relative importance of the listed factors. The reference to any novel or innovative applications of technology includes hardware (i.e., cameras), software (i.e., artificial intelligence or algorithmic decision making), biometrics, and more. Several of the factors address the possibility of the creation of new information collections or the formation of new databases that merge records otherwise maintained separately in federal, state, or private hands.

The third paragraph provides that the Director of OMB must issue guidance on the PIA process. The guidance should help agencies (A) decide whether to conduct a thorough or limited PIA assessment process; (B) establish priorities for conducting PIA assessment processes; (C) address privacy as part of other information management functions, including information and information system life cycles; other requirements relating to the collection of information; and information system development, security, and use of technology resources; (D) determine when and how to conduct public consultations; (E) conduct a PIA process that involves more than one agency; and (F) conduct any other aspect of the PIA process.

This provision gives OMB a significant responsibility and considerable discretion. It recognizes that privacy management is part of information management activities and regulatory controls over agency information activities, which are not limited to personally identifiable information activities. Privacy management needs to fit into and be part of overall information management responsibilities and not a separate activity unrelated to other requirements. This supports the existing goal of better integration of privacy within information and technology management.[228]

[228] See, e.g., Paperwork Reduction Act, 44 U.S.C. § 3506, https://www.law.cornell.edu/uscode/text/44/3506; Office of Management and Budget, Managing Information as a Strategic Resource (2016) (Circular A-130).

3. Managing the PIA Process

(c) MANAGING THE PRIVACY IMPACT ASSESSMENT PROCESS.

(1) The Chief Privacy Officer shall determine the scope of each privacy impact assessment process, including deciding whether a thorough or limited process is appropriate; which agency activities affecting privacy should be included in which privacy impact assessment process; identify the agency components that shall participate in the process; establish a timetable for the process; and manage any public notice and public participation.

(2) Each privacy impact assessment process shall result in a final written report.

(3) If an agency activity affecting privacy involves classified information or other information unsuitable for public disclosure under existing laws and Executive Orders, the agency shall disclose publicly as much about the privacy impact assessment process as practicable.

(4) If in the judgment of the Chief Privacy Officer, it is not practical to complete a privacy impact assessment process before an agency begins or significantly changes an activity that would otherwise require a privacy impact assessment process, the Chief Privacy Officer may delay or otherwise adjust the conduct of the process and the timing and form of public report in a suitable manner. The Chief Privacy Officer shall provide public notice of any delay or adjustment on the agency privacy website.

(5) The Chief Privacy Officer shall send to appropriate Committees of Congress a copy of each interim and final written report on each major privacy impact assessment.

Subsection (c) addresses management of the PIA process, placing the agency CPO in charge. The CPO determines the scope of each PIA process, including whether a thorough or limited PIA process is appropriate; which A3Ps fall within a PIA process; which agency components should participate in the process; the timetable for the process; and the public notice and public participation part of the effort. That is a lot of authority and responsibility, and it requires someone with a modest degree of independence from the activity being assessed. If the same people responsible for an activity also run the PIA process, there may be insufficient objectivity or willingness to make the process useful. When major disagreements break out among agency components with an interest in a PIA process, the ability of the CPO to take a major issue directly to the head of the agency may come into play. See section (9)(e)(1).

Paragraph (2) states that a final written report is a part of the process, and paragraph (3) makes clear that the report should be public unless parts are classified or unsuitable for public disclosure under existing laws and Executive Orders. An agency cannot make up a new reason for withholding the report that is not firmly rooted in an existing law or policy addressing confidentiality. Except in narrow circumstances – e.g., when an activity is classified in its entirety – some elements of a report should be available for public disclosure.

Paragraph (4) addresses the difficult problem of the timing of the PIA process. There may be circumstances requiring that an activity begin operations (or implement changes to an existing activity) before the agency can complete the PIA process. The agency CPO manages the timing of the process and public reporting on the process. The CPO can hold up an activity when appropriate in order to make public disclosure and seek public input. An agency component should not be rewarded if it delays elements of the PIA process, but at the same time, agency operations should continue in an appropriate and efficient manner. The tradeoffs here can be difficult, and the CPO must resolve them.

Paragraph (5) requires that the agency CPO send copies of each interim and final report on a PIA process to appropriate congressional committees. This means oversight committees, including the

committees that originated the USA FIPS Act, authorizing committees that produced the legislation for the programs, and appropriations committees that approve funding. There may be other committees with an interest as well.[229]

4. Elements

(d) ELEMENTS OF A PRIVACY IMPACT ASSESSMENT PROCESS.

(1) An agency conducting a thorough privacy impact assessment process shall, to the extent practicable, include –

(A) an identification of risks to the agency from the processing of records, including a description of ways to manage and to mitigate the risks and a justification for the final choices made by the agency;

(B) an identification of information technology available to support the processing of records, including a justification for the final choices made by the agency;

(C) an analysis of the risks and consequences of the activity for privacy of data subjects, including expected uses and disclosures; a description of possible ways to mitigate the consequences and risks; and a justification for the final choices made by the agency; and

(D) a description of efforts to seek public and stakeholder participation in the privacy impact assessment process and a response by the agency to public and stakeholder comments.

(2) An agency conducting a limited privacy impact assessment process shall, to the extent practicable, include –

(A) an explanation of the reasons that the agency decided to conduct a limited rather than a thorough privacy impact assessment process;

(B) a description of the risks and consequences of processing of records for the agency and for data subjects;

(C) a description of alternatives considered;

(D) a justification for the final choices made by the agency; and

(E) a summary of any public and stakeholder participation and comments.

Subsection (d) sets out the elements of a thorough and a limited PIA process. In both cases, the proposal says *to the extent practicable*. This intentionally gives some discretion to the agency CPO to adjust a PIA process to the nature of the activity, the needs of the agency, and the resources and time available for conducting a PIA process.

There are four elements to a thorough PIA process. First, the process should identity the risks to the agency from the processing of records. This includes describing ways to manage and to mitigate the risks and a justification for the final choices made by the agency. In other words, the process should not just be descriptive but should identify what alternatives the agency considered and how and why the agency made decisions between the choices identified. The process should be similar to an exam that asks a student to produce an answer and to show the way that the answer was achieved.

---

[229] The practice of identifying committees in legislation by name creates an obligation to amend the legislation later when committee names change. The "appropriate committee" approach avoids the need for these amendments, but it relies on the good faith of the CPO to identify the relevant committees. Congressional committees that feel slighted because an agency failed to inform them about a PIA report can find their own ways to express displeasure.

Second, the process should identify the information technology available to support the processing of records, including a justification for the final choices made by the agency. As with the first element, this one requires the agency to show the alternatives considered and to justify its final choice.

Third, a thorough process should analyze the risks and consequences of the activity for privacy of data subjects, including expected uses and disclosures and a description of possible ways to mitigate the risks and consequences and a justification for the final choices made by the agency. A focus here should be on looking for ways to limit uses and disclosures. In particular, this means making sure that each agency designated disclosure is both necessary and as narrow as possible.

Finally, the process should describe efforts to seek public and stakeholder participation in the assessment, including a response by the agency to public and stakeholder comments. This element emphasizes the importance of public and stakeholder participation. An agency has considerable discretion to determine how to involve the public and stakeholders in the assessment, and here too, the agency must explain and justify its choices. As with a formal notice and comment process, the agency should explain why it did or did not adopt suggestions that it received.

A limited PIA process has five elements that are less intensive than the elements required for a thorough assessment. First, the agency must explain why it chose a limited assessment. Second, the agency must describe the risks and consequences of the processing. Presumably, the stakes in an activity that qualifies for a limited assessment will be lower than for activities that receive a thorough assessment. Third, the agency must describe alternatives considered. Fourth, the agency must justify the final choices. Finally, the agency must summarize agency and stakeholder participation and comments.

A limited PIA process might be used when processing is narrow and where the stakes are limited. An A3P that collects parking permit data from agency employees would likely qualify for a limited process. Also, a modest change to an existing A3P – such as the addition of a new ADD because of a new statutory requirement – might also be addressed through a limited PIA process. Small substantive changes to an A3P might call for a limited PIA process with a report that might be a page or two. Descriptive or similar minor changes might not require any PIA.

5. Public Notice and Participation

(e) PUBLIC NOTICE AND PARTICIPATION. The Chief Privacy Officer of an agency shall, to the extent practicable, provide for public notice of each privacy impact assessment process and for public comment or other public participation in the process. The Chief Privacy Officer may provide public notice through the privacy website of the agency or through the Federal Register.

Subsection (e) provides that the CPO must provide for public notice of each PIA process, as well as for public comment or other public participation in the process. With a major A3P, especially one affecting many members of the public, the process might warrant public hearings of some type or public listening sessions with stakeholder and issue advocates, with industry, and perhaps with technology experts. The agency CPO has considerable discretion to design the role and timing of public and stakeholder participation. The timing of that participation is important. It will only be valuable if done as early in the decision-making process as possible. If the design of an activity changes in the course of planning, there could be a need for more than one round of public participation.

Major new systems and controversial uses of technology will most likely call for greater participation. Stakeholders can include the public, other agencies, and private companies that have an interest in the activity. The requirements for notice and participation are modified by the now familiar words *to the extent practicable*. This recognizes that one size will not fit every activity and that time and resources are limited. Hard choices may be necessary, but the discretion allowed should not be taken as an excuse for avoiding input from outside the agency.

The importance of public participation cannot be overemphasized. In one instance, an agency developed the use of a new technology and a new Privacy Act system of records that was expected to affect many members of the public on a routine basis. I observed and participated in an early and informal (and off-the-record) listening session between the agency planners and representatives from the privacy community. The result of the discussion was a significant change in design that made the program both more effective and less intrusive. At the end of the process, the agency representative thanked the privacy community for its input and expressly acknowledged the valuable assistance provided. The emphasis in the bill for consultations recognizes that agencies do not necessarily know everything that they should know or need to know when planning activities. Other perspectives can produce results that may be better for the agency and for data subjects.

Part of the discretion allowed to the CPO is how to engage the public. Federal Register notices are a traditional way of providing public notice, but an agency must choose to use the agency's privacy website either instead of or in conjunction with a Federal Register notice. For example, a Federal Register notice might direct interested parties to the agency website where relevant documents and other materials will be found. A limited PIA process may call for only the most minimal public participation, perhaps through a website notice inviting public comment. Nothing prevents a CPO from reaching out in other ways to find and engage interested stakeholders.

6. E-Government Act

(f) PUBLIC LAW 107-437. – An agency or component that completed the transition to this Act shall not comply with section 208 of Public Law 107-437, 44 United States Code § 3501 note.

Finally, as noted above, the existing PIA requirement in the Electronic Government Act of 2002 leaves much to be desired. The bill provides that an agency that completed the transition from the Privacy Act to the USA FIPS Act cannot comply with the existing requirement. The agency must use the new requirement and cannot choose to use the old one instead.

A provision in Section 20 of the USA FIPS Act addresses how an agency should conduct a PIA process during the period of transition from compliance with the Privacy Act to compliance with the USA FIPS Act.

L. Exemptions (Section 12)

The exemptions in the Privacy Act of 1974 are inconsistent, procedurally cumbersome, and administratively difficult. The earlier discussion of Privacy Act exemptions reviews many of these matters. However, it appears that the exemptions protect most governmental interests that need protection. I do not recall any formal proposals to expand the exemptions in my years of involvement with the Privacy Act. By contrast, over the years, proposals for new exemptions to the Freedom of Information Act are not unusual. Still, the exemption for the CIA alone among intelligence agencies is

an issue, and the *travelling exempt record* problem has a working solution that stands on somewhat shaky grounds.

The exemptions may be too broad in some instances, and it appears that agencies do not always take the position that exempt information must always be withheld in its entirety. When particular information sought by a data subject is exempt but the need for protection is nonexistent, some agencies release that information some of the time. It is impossible to quantify the extent to which this happens.

The USA FIPS Act consolidates all exemptions in Section 12 rather than repeating the Privacy Act's pattern of scattering exemptions in various places. For the most part, the proposal continues existing exemptions, but because of the convoluted way that the existing (j) exemptions appear (exempting some systems of records from any part of the Privacy Act *except* selected provisions), there are some technical changes there. Also, a few existing exemptions no longer seem needed. The discussion here explains the changes.

1. Limits

(a) LIMITS ON ACCESS. – Nothing in this Act shall allow an individual a right of access to a record or a disclosure history record, or a right of amendment of (1) any information compiled in reasonable anticipation of a civil action or proceeding, (2) any classified information; (3) data or information acquired by an agency under a pledge of confidentiality and used or disclosed for exclusively statistical purposes pursuant to section 3572 of title 44, United States Code; (4) any information created as testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if disclosure would compromise the objectivity or fairness of the testing or examination process; or (5) information that was exempt from disclosure under section 552a of title 5, United States Code, as information collected prior to the effective date of section 3 of the Privacy Act of 1974 (Public Law No. 93-579) under an implied promise that the identity of the source would be held in confidence.

Subsection (a) of Section 12 includes the two unlabeled exemptions contained in the Privacy Act. One is for attorney work product information and the other is for classified information. In both instances, nothing in the USA FIPS Act requires an agency to provide an individual a right of access, amendment, or a disclosure history. Another existing and more "classical" specific exemption in the Privacy Act covers systems of records "required by statute to be maintained and used solely as statistical records."[230] Because an exemption for these records is only appropriate for the access and amendment provisions, that exemption fits well here. The same is true for testing or examination material used in the civil service if disclosure would compromise the process.[231]

---

[230] 5 U.S.C. § 552a(k)(4).

[231] In addition to the access and amendment exemption, the Privacy Act exempts testing or examination material from the requirement to process only relevant and necessary information. The need for that exemption is unclear, and the bill removes it. The purpose of the testing exemption, as identified in the OMB Guidelines, is to protect written examinations that cannot "be revised in their entirety each time they are offered." 40 Federal Register 28948-79, at 28974. If that were the only interest relevant, then an exemption from access and amendment would be sufficient. But the Guidelines also suggest that "This language also covers certain of the materials used in rating individual qualifications." Id. Further, there is at least one case using the exemption for evaluation materials. See Robinett v. USPS, cited in the Department of Justice, Overview of the Privacy Act of 1974 at 306. It is not clear,

The provision also continues protections for information collected before the effective date of the Privacy Act (September 27, 1975) for information obtained at a time when there was no requirement for express promises of confidentiality. The need to continue this protection is marginal. At best, any of these sources provided information probably fifty or more years before the effective date of the USA FIPS Act. This exemption is here just in case there are still some sources that warrant protection.

2. Personnel Information

(b) PERSONNEL INVESTIGATIONS AND EVALUATIONS. – An agency is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record with respect to any information that would identify a confidential source who furnished information to the Government under an express promise that the identity of the source would be held in confidence if the information was created as –

(1) investigatory material solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information.

(2) evaluation material to determine potential for promotion in the armed services.

Subsection (b) consolidates the federal personnel exemptions from subsection (k) of the Privacy Act for investigations and evaluations. As with existing law, the main purpose is to protect those who provided information under an express promise of confidentiality. These are precisely the same interests that the current exemptions protect. The exemptions are from the rights for access, amendment, and disclosure history. The provision also continues an exemption from the requirement to process only relevant and necessary information (now in subsection (a) of section 4. That exemption remains appropriate for investigations and evaluations because it is not always clear what information will be relevant or necessary to those processes.

3. Law Enforcement

(c) INVESTIGATORY MATERIAL FOR LAW ENFORCEMENT PURPOSES. –

(1) An agency is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record, for investigatory information compiled for law enforcement purposes unless the individual is denied any rights, benefits, privileges, or status that the individual would otherwise be entitled to by Federal law, or for which the individual would otherwise be eligible, as a result of the maintenance of the information.

(2) Any right of access, right of amendment, or a disclosure history record in section 7 and section 8 that an individual would have as a result of a denial of any rights, benefits, privileges, or status as described in paragraph (1) of this subsection shall not apply to –

(A) the extent that the disclosure of the material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence;

(B) information exempt from disclosure pursuant to subsection (a)(5) of this section; or

---

however, that the application in the Robinett case to evaluation material was appropriate, as evaluation material is not expressly mentioned in (k)(6) as it is in exemption (k)(7) covering the armed services.

(C) information that qualifies for exemption as criminal law enforcement information in subsection (f).

Subsection (c) is a replacement for the (k)(2) exemption in the Privacy Act. The provision exempts investigatory information compiled for law enforcement purposes from the requirement to process only relevant and necessary information. In addition, it includes an exemption from rights of access, amendment, and disclosure history but this exemption applies only if an individual was denied a right, benefit, privilege, or status as a result of the maintenance of the information. However, protections for sources who provided information under an express promise of confidentiality that exist in current law remain in place. The only modest substantive change is the addition of the word *status* to right, benefit, and privilege. The rights of access, amendment, and disclosure history granted under the limitation do not apply to information obtained prior to the effective date of the Privacy Act under an implied promise of confidentiality as to the identity of the source of the information, or to information subject to the exemption in subsection (f) for criminal law enforcement information.

As with the Privacy Act, the exemptions in subsection (c) cover material compiled for an investigative law enforcement purpose. That purpose can be civil or criminal. The criminal component here only applies to law enforcement agencies that are not principally criminal law enforcement agencies. Subsection (f) covers those agencies. The exemption here does not apply to material compiled solely for routine background investigations for security clearances. Subsection (b) covers employment related investigations, including for clearances. The discussion in this subsection does not change existing interpretations of the Privacy Act.

4. Protective Services

(d) PROTECTIVE SERVICES. –An agency activity affecting privacy operated by an agency in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18, United States Code, is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record to the extent that records in the agency activity affecting privacy relate to those protective services.

Subsection (d) covers protective services for the President and others. It continues the existing Privacy Act exemption from the requirement to process only relevant and necessary information and from rights of access, amendment, and disclosure history. As with current law, the limit on the exemption for denial of rights, benefits, and privileges does not apply here. Protective functions straddle the line between law enforcement and criminal law enforcement activities. Because the USA FIPS Act allows agencies broad discretion to decide what functions to include in an A3P, additional language here makes it clear that the exemption only applies to records that relate to protective services. An agency cannot add other functions to an A3P and then claim the exemption for functions unrelated to protective services.

5. Intelligence Agencies

(e) INTELLIGENCE AGENCIES. –
(1) An intelligence agency or component thereof defined as part of the Intelligence Community pursuant to section 3003, title 50, United States Code is exempt from –

(A) the requirements to comply with subsections (a), (b), (c), and (d) of section 4; and
(B) the requirements in section 7 and section 8 to provide an individual a right of access, right of amendment, or a disclosure history record.

Subsection (e) expands on the CIA exemption in (j)(1) of the Privacy Act by extending the same exemption to any intelligence agency or component identified pursuant to 50 U.S.C. § 3003. That provision is currently implemented through Executive Order 12333. The Privacy Act states the CIA exemption in a negative way, but subsection (e) states the exemption affirmatively. It only names those provisions of the Act for which the bill allows an exemption. The effect is to remove the possibility for exemptions from irrelevant provisions of the Act. The exemptions affirmatively provided cover the requirements for relevant and necessary processing; direct collection; notice at time of collection; and accuracy, relevance, timeliness, and completeness. These are in section (4)(a)-(d) of the USA FIPS Act. There is also an exemption from the right of access, amendment, and disclosure history. These exemptions cover the core needs of intelligence agencies. There is no exemption from requirements to publish descriptions of A3Ps or agency rules. The requirement for publishing descriptions of all A3Ps continues the core philosophy of the Privacy Act that no agency should maintain secret records systems hidden from the public. As with existing law, there is no intelligence agency exemption from the limit on collecting records about First Amendment activities.

6. Criminal Law Enforcement Agencies

(f) CRIMINAL LAW ENFORCEMENT AGENCIES. – A criminal law enforcement agency or component thereof that performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, is exempt from the requirement to comply with subsections (a), (b), (c), and (d) of section 4, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record with respect to any records that consist of –
(1) 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;
(2) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or
(3) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

Subsection (f) provides an exemption that is the equivalent of the Privacy Act's (j)(2) exemption for criminal law enforcement activities. As with the existing provision, the proposed exemption is available only to a criminal law enforcement agency or component thereof that performs as its principal function any activity pertaining to the enforcement of criminal laws. The case law here reflects some confusion by the courts. For the criminal law enforcement exemption to apply, the enforcement of criminal law must *the* principal – meaning primary – function of the agency or component. An agency with two principal functions cannot use this exemption if only one of those functions is an activity pertaining to the enforcement of criminal laws. Many agencies meet the threshold requirement here, including the FBI and the DEA. The IRS is not principally a criminal law enforcement agency, but its Criminal Investigation Division qualifies as a component whose principal function is enforcement of criminal law. Similarly, Offices of Inspectors General have multiple functions that include enforcement of criminal laws as one of those functions, but criminal law

enforcement is not the principal function of an IG.[232] An A3P operated by a criminal investigation unit within an IG's office can qualify, however.

Once the threshold requirement is met, a record is only exempt if it falls within one of three categories of information compiled for a specific purpose. The proposal repeats the language in the Privacy Act without change. Here too, there is case law that ignores the requirement that records fall within one of the three specified categories. The reenactment of the provision unchanged should not be read as supporting that line of cases. Given the potential breadth of an A3P under the USA FIPS Act, it is crucial that records meet all the requirements in order to qualify for an exemption. An agency may choose to include within a single A3P records that qualify along with records that do not qualify. However, only those records falling within one of the three categories qualify for exemption.

7. National Archives

(g) NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. – Any record subject to this Act accepted by the National Archives of the United States as a record with sufficient historical or other value to warrant its continued preservation by the United States Government pursuant to section 2107 of title 44, United States Code, and that the Archivist of the United States processes pursuant to section 2108 of title 44 United States Code, shall not be subject to any of the requirements of this Act.

Subsection (g) exempts from the USA FIPS Act records accepted by the National Archives for historical preservation or otherwise under 44 U.S.C. § 2107. As explained in the discussion of the exemptions in the Major Issues section of this report, the exemption is slightly modified from the Privacy Act. Current law still applies the publication requirement of the Privacy Act. However, other laws fulfill the purpose of the publication requirement so the requirement is unnecessary.

8. General Requirements

(h) GENERAL REQUIREMENTS. –

(1) When publishing a notice of an agency activity affecting privacy that includes a record exempt or potentially exempt under provisions of this section, an agency shall, to the extent practicable, describe the activities that qualify for the exemption and distinguish exempt and non-exempt records and activities. The agency shall include in the notice the reasons the agency expects to utilize the exemptions.

(2) In applying an exemption available under this section, an agency shall restrict application of the exemption to those records and activities that include information that the exemption seeks to protect.

(3) If an agency discloses a record exempt under this section from any provision to another agency, the record shall continue to be exempt in the same manner and to the same extent as if the disclosing agency continued to process the record. An agency transferring an exempt record shall identify for the recipient agency the part of the record that qualifies for exemption and the nature and scope of the exemption.

---

[232] See generally, the Inspector General Act of 1978, 5a U.S.C. § 3, https://www.law.cornell.edu/uscode/text/5a/compiledact-95-452/section-3.

Subsection (h) seeks to limit the actual application of exemptions in practice. First, it provides that an agency must in its A3P notice describe its activities that qualify for an exemption and distinguish exempt from non-exempt records and activities. This notice obligation applies to the extent practicable. It may not be possible in a general notice to delineate all lines between exempt and non-exempt records when both types are part of the same A3P. Of course, it might be better to have exempt records in their own A3P. However, that may not always be possible or practical, especially when an A3P has only occasional exempt records. An A3P that has exempt records must include in the published notice the reasons the agency expects to use the exemptions. This will inform the public why records may be exempt and how to distinguish between exempt and non-exempt records.

Second, when invoking an exemption, an agency must restrict application of the exemption to those records and activities that include information that the exemption seeks to protect. This underscores that an agency must specifically justify its use of exemptions when actually applying the exemptions and not just when publishing an A3P notice. However, where records are exempt because of maintenance by an intelligence agency, criminal law enforcement agency, or protective services agency, the agencies are not obliged to review individual records or parts of records to determine the relevance of an exemption. When they apply, these exemptions are categorical, although as subsection (i) makes clear, an agency can waive exemptions.

Third, the USA FIPS Act expressly addresses the problem of the travelling exempt record by providing that an exempt record retains its exempt status when disclosed to another agency. The exemption in the hands of the recipient agency is precisely the same as if the disclosing agency still maintained the record. A different exemption may possibly apply to the records in the hands of the recipient agency, and a recipient agency may also apply that different exemption to that record when applicable. An agency providing an exempt record to another agency must identify the part of the record that qualifies for exemption as well as the nature and scope of the exemption. Failure to provide the proper identification does not cancel the exemption, however.

9. Waivers

(i) WAIVERS. – An agency processing a record that qualifies for exemption in this section may take one or more of the following actions –

(1) waive application of an exemption, in whole or in part, by including the waiver in the description required in section 5(c) of an agency activity affecting privacy;

(2) issue a regulation defining when the agency may waive application of an exemption, in whole or in part; and

(3) waive application of an exemption in whole or in part or on a case-by-case basis.

Subsection (i) expressly authorizes an agency to waive an exemption either in the description of an A3P, by issuing a regulation, or through case-by-case decisions. This provides agencies with great flexibility to waive exemptions when records do not need the protections available. This provision resulted in part from a review of the CIA's regulation formally waiving Privacy Act exemptions discussed above. Other agencies waive exemptions as well from time to time. However, it would be challenging to provide statutory standards for waiving exemptions and any attempt to do so would just create opportunities for additional litigation. The better alternative is to give agencies express authority to do so without a mandate to do so. Essentially, subsection (i) gives agencies a free hand to waive exemptions as they see fit. Of course, other laws and policies that prohibit discriminatory practices continue to apply. It would be improper to waive exemptions for men but not women, for

example. Otherwise, the objective is to give agencies broad discretion as well as encouragement to waive the use of exemptions when the exemptions are not needed in fact.

****

In some instances, the Privacy Act allows agencies to exempt a system of records from the civil remedies provision of the Act. This is a particularly unusual type of exemption that appears to deny any possibility of a judicial remedy. The courts often avoid giving this provision the broad application that it appears to have. At least one agency (Housing and Urban Development) – and perhaps others – did not invoke this exemption even though it could have. The responsible official reportedly said at the time that the agency should be held accountable for compliance with the Privacy Act. That is the approach taken here. The USA FIPS Act allows no exemption from civil remedies.

M. Criminal and Other Penalties (Section 13)

The criminal penalties of the Privacy Act have not been effective in deterring violations. In some respects, this is not surprising. The penalties are misdemeanors with $5000 fines, and prosecutors have little interest in these cases. In addition, it can be difficult to pin responsibility on an individual functioning in a bureaucratic setting. Who could be held criminally responsible for operating a system of records without meeting the notice publication requirement? The agency head? Program manager? Program staff? Privacy Act officer? In any event, while there may be a role for criminal penalties in bureaucratic government, criminal law may not provide the best incentive for compliance.

1. Offenses

(a) OFFENSES. –
(1) Any person who knowingly and in violation of this Act and under false pretenses obtains a record that contains personally identifiable information shall be punished as provided in subsection (b).
(2) Any officer, employee, contractor, grantee, or volunteer of an agency, or other person who by virtue of employment, official position, or contract has possession of, or access to, a record that contains personally identifiable information the disclosure of which is prohibited by this Act or by rules or regulations established thereunder, and who knowing that disclosure of the record is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be punished as provided in subsection (b).

Subsection (a) of section 13 defines two crimes similar to existing Privacy Act crimes but with stiffer penalties. The first is for seeking a record under false pretenses. An individual who improperly seeks a record about another individual might violate this provision. The second crime is for disclosing a record in violation of the Act. The new provision makes it clear that contractors, grantees, volunteers, and other persons who have legitimate access to a record can be found guilty of improper disclosure as can officers and employees already expressly covered by the existing provision.

2. Penalties

(b) PENALTIES. – A person described in subsection (a) shall –
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed with intent to sell, transfer, or use a record that contains personally identifiable information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

The penalties in subsection (b) are similar to penalties in HIPAA for wrongful disclosure of individually identifiable health information.[233] The basic penalty is a fine up to $50,000, imprisonment up to a year, or both. Enhanced penalties apply if an offense is committed with intent to sell, transfer, or use a record for commercial advantage, personal gain, or malicious harm. Penalties can range up to $250,000, ten years in prison, or both. These are significant penalties when an individual improperly obtains or discloses PII.

3. Publishing

(c) PUBLISHING. – Any officer or employee of any agency who willfully establishes or maintains an agency activity affecting privacy without meeting the requirements in section 3 to publish a description of the agency activity affecting privacy shall be guilty of a misdemeanor and fined not more than $5,000.

Subsection (c) continues the misdemeanor penalty in the Privacy Act for maintaining an agency activity affecting privacy without publishing the requisite notice. I proposed to eliminate this crime entirely. However, agency Privacy Act officers said that while this penalty may be largely unenforceable, it was effective in convincing program officials that they must comply with the requirement to publish a notice. That is the only reason this provision remains. Subsection (d) provides for adverse personnel action against a violator, and that provision overlaps with the crime in subsection (c). Adverse personnel actions may actually provide a better incentive than criminal law to encourage compliance.

4. Adverse Personnel Actions

(d) ADVERSE PERSONNEL ACTIONS. – An officer or employee of an agency who processes records in violation of this Act shall be subject to appropriate administrative discipline including, when circumstances warrant, suspension from duty without pay or removal from office.

Subsection (d) provides that an agency officer or employee who processes records in violation of the USA FIPS Act shall be subject to appropriate administrative discipline including, when circumstances warrant, suspension from duty without pay or removal from office. This language is modeled on two provisions in title 31. One provides for adverse personnel actions against those who authorize an expenditure or obligation in violation of law.[234] The other provision similarly penalizes those who exceed limitations on expending and obligating amounts in excess of appropriations.[235]

---

[233] 42 U.S.C. § 1320d-6, https://www.law.cornell.edu/uscode/text/42/1320d-6.

[234] 31 U.S.C. §§ 1517, 1518, https://www.law.cornell.edu/uscode/text/31/1517, https://www.law.cornell.edu/uscode/text/31/1518.

[235] 31 U.S.C.§§ 1349, 1341, 1342, https://www.law.cornell.edu/uscode/text/31/1349, https://www.law.cornell.edu/uscode/text/31/1341, https://www.law.cornell.edu/uscode/text/31/1342.

N. Government Contracts, Grants, and Cooperative Agreements (Section 14)

When an agency provides by a contract, grant, cooperative agreement, or otherwise for the conduct of an agency activity affecting privacy to accomplish an agency function, whether in whole or in part, the agency shall, consistent with its authority, cause the requirements of this Act to be applied to the activity. The agency shall be responsible for any publication, notice, or rule required under this Act with respect to that agency activity affecting privacy.

Subsection (m) of the Privacy Act says that when an agency provides by contract for the operation by or on behalf of the agency to accomplish an agency function, the agency must apply the provisions of the Act to the contract. Other language in the subsection makes clear that criminal penalties in the Privacy Act apply to employees of the contractor.

Section 14 is a substitute for the existing provision and has many similarities.[236] The basic requirement is the same, and the standard is the same. A major difference is that the new language applies not just to contracts but also to grants, cooperative agreements, or other arrangements where an agency provides for the operation of an A3P to accomplish an agency function. Agencies sometimes use instruments other than contracts to hire others to accomplish an agency function, and the new language closes that loophole. The substance of the arrangement should determine if the USA FIPS Act applies, not the form of the agreement. The language in subsection (m) about criminal penalties does not appear in section 14. The criminal penalties in section 13 apply criminal penalties to contractors, grantees, and others who violate the law.

The basic idea of section 14 is the same as with the Privacy Act. The person operating the A3P for the agency must be doing so to accomplish an agency function. It is not a simple matter of the use of federal funds by a third party. If an agency grant provides funds for a function that includes the maintenance of records about individuals, that grant would not be subject to the requirement in Section 14 unless the function is one that the agency would or could carry out for itself and the grant calls for the maintenance of those records for the agency. If an agency provides funds to a state or local government to support or manage an activity by that government, section 14 will not apply because the function is not one that the agency would perform. The agency's function here is

---

[236] The 1975 OMB Guidelines on the Privacy Act explaining the subsection (m) provision remain relevant here. But for the broadening of application to other instruments, the new provision is the same. For both provisions, the lines drawn are occasionally unclear and require the exercise of judgment to determine whether a privacy requirement belongs in the contract or other instrument. ("While the contract need not have as its sole purpose the operation of such a system, the contract would normally provide that the contractor operate such a system formally as a specific requirement of the contract. There may be some other instances when this provision will be applicable even though the contract does not expressly provide for the operation of a system; e.g., where the contract can be performed only by the operation of a system. The requirement that the contract provide for the operation of a system was intended to ease administration of this provision and to avoid covering a contractor's system used as a result of his management discretion. For example, it was not intended that the system of personnel records maintained by large defense contractors be subject to the provisions of the Act.") 40 Federal Register 28948-79, at 28976 (July 9, 1975), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/OMB/inforeg/implementation_guidelines.pdf.

awarding funds to another government to manage an activity of that government.[237] As with the Privacy Act, requirements of the USA-FIPS Act do not simply follow federal funds. If a federal agency contracts with a company to pave a road and the company hires employees and maintains records about those employees, neither subsection (m) of the Privacy Act nor section 14 of the USA-FIPS Act would apply to those records. The contract does not directly require the maintenance of records about employees for the agency. If an agency gives a grant to a university for medical research, that would not qualify as an agency function even if the agency carries out some research on its own. The specific research covered by the grant is not an agency function even though other research may be. However, if an agency awarded a grant for data collection that would be input to an agency research project, that grant would fall under section 14.

Subsection (m) of the Privacy Act includes a provision stating that a consumer reporting agency is not a government contractor if an agency reports a claim under 31 U.S.C. § 3711(e). That language was not necessary under the Privacy Act because a consumer reporting agency neither maintains a system of records for a government agency nor does it carry out a government function. The USA FIPS Act drops the language solely because it is unnecessary.

O. Matching (Section 15)

The computer matching provisions in the Privacy Act have two main parts. One part installs administrative controls over matching activities involving federal agencies. The USA FIPS Act make modest adjustments to the administrative controls. The second part provides due process protections to individuals identified as a result of a matching program. The draft bill leaves the due process elements of matching largely unchanged.

The goal of the due process provisions was to prevent agencies (federal, state, or local) from taking action against an individual solely on the basis of the results of matching. The law requires notice to the individual and verification of information before using it to suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to the individual, or take other adverse action against the individual. The importance of due process is just the same as it was decades ago.

One of the controls in the Privacy Act comes from Data Integrity Boards (DIB). The Privacy Act requires each agency involved in matching to establish a DIB to review and approve matching activities. It is not apparent that the DIBs remain useful, if they ever were. At some agencies, the approval process is a "paper" activity, with matching agreements circulated for signature rather than for discussion at a DIB meeting. That process has little value because each office involved in matching simply approves what another office proposes so that its own matching activity will be approved. There is no tension or incentive for serious review. There is no evidence that the role of DIBs

[237] In *Schapiro v. Koch*, 777 F. Supp. 2d 86 (D.D.C. 2011), https://www.courtlistener.com/opinion/2476621/koch-v-schapiro/, a court refused to apply the Privacy Act to a contract "for the design or development of a system of records; it was a contract to investigate complaints of discrimination by employees of the agency on behalf of the SEC's EEO Office." That decision was incorrect in applying the *agency function* standard. It is not the basic design or development of a record system that matters. In that case, investigating complaints of discrimination by employees was the agency function. Records maintained by a contractor for that purpose should fall under subsection (m) of the Privacy Act and under Section 14 of the USA FIPS Act.

expanded into other privacy areas. As a result, there is no good reason to continue DIBs. Instead, the USA FIPS Act expands the role of the agency CPO in the matching process.

The discussion below highlights significant changes to matching proposed in the USA FIPS Act and does not dwell on provisions that remain substantially similar to those in the Privacy Act.

1. Matching Agreements

(a) MATCHING AGREEMENTS. –

(1) CONTENTS OF MATCHING AGREEMENTS. – A source agency shall not disclose a record processed as part of an agency activity affecting privacy for use in a matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency receiving the records, specifying –

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings resulting from the operation of the program;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter. to data subjects whose records are used in the activity that any information provided by the data subjects may be subject to verification through matching programs;

(E) procedures for verifying information produced in the matching program as required by this section;

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in the matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of the programs;

(H) prohibitions on duplication and redisclosure of records imposed by the source agency on the recipient agency or the non-Federal agency, except where duplication or redisclosure is required by law or essential to the conduct of the matching program;

(I) procedures governing the use by the recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return or destruction of the records used in the program;

(J) information on assessments that have been made on the accuracy of the records that will be used in the matching program;

(K) that the Comptroller General may have access to all records of a recipient agency or non-Federal agency receiving the records as the Comptroller General deems necessary in order to monitor or verify compliance with the agreement;

(L) a provision requiring revision or termination of the agreement if the need for, circumstances relating to, or the law regarding any aspect of the matching agreement changes in a material way during course of the agreement; and

(M) the expiration date for the agreement, which can be no later than five years after the agreement took effect.

(2) CERTIFICATION OF MATCHING AGREEMENT. – No matching agreement shall take effect unless the Chief Privacy Officer of the source agency certifies in writing that –

(A) the agreement complies with all requirements of this Act;

(B) the Chief Privacy Officer of the source agency consulted with the agency Inspector General, Chief Information Officer, Chief Data Officer, and senior officials from the office providing or using records for the matching program activity about the justification for the matching program;

(C) any findings of the agency Inspector General or the Government Accountability Office relevant to the matching program were adequately taken into account in the agreement;

(D) any problems identified in previous matching programs between the same agencies were adequately addressed;

(E) except for matching programs mandated by statute, in the judgment of the Chief Privacy Officer of the source agency, the sharing of records pursuant to the matching agreement is financially justified based on any relevant results of current or past matching programs; and

(F) except for matching programs mandated by statute, in the judgment of the Chief Privacy Officer of the source agency, the matching program is in the public interest.

(3) PRIOR COMPLIANCE REQUIRED. – No source agency may enter into a second or subsequent matching agreement unless –

(A) the recipient agency or non-Federal agency receiving the records certifies that it complied with the provisions of previous agreements; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(4) POSTING. – A copy of each matching agreement and a copy of the certification of the Chief Privacy Officer shall be posted on the website of the source agency and sent to the Director of the Office of Management and Budget.

(5) EFFECTIVE DATE OF AGREEMENT. – No matching agreement shall be effective until 30 days after the date on which a copy is posted on the agency website.

(6) SECTION NOT AUTHORITY TO CONDUCT PROGRAMS. – Nothing in this section may be construed to authorize –

(A) any matching programs not otherwise authorized by law; or

(B) disclosure of records for a matching program except to a Federal, State, or local agency.

Paragraph (a)(1) sets out the requirement content of a matching agreement between a source agency and a recipient agency or non-Federal agency. Most are the same as current law. Subparagraph (L) addresses the need for revision or termination language in an agreement in case of material change during the course of an agreement. The possibility of revision or termination is important because matching agreements can, as provided in subparagraph (M), last five years. This replaces the current period of 18 months with the possibility of a one-year extension. That relatively short period created unnecessary paperwork.

Paragraph (a)(2) imposes on the agency CPO a responsibility to certify in writing that a matching agreement compiles with all requirement of the USA FIPS Act. When the agency is a source agency, the CPO must also certify that the CPO consulted with the agency Inspector General, CIO, and Chief Data Officer, as well as with senior officials from the office providing or using records about the justification for the matching program. This is a partial substitute for the existing requirement, often ignored, that agencies assess the costs and benefits of matching activities. The CPO must also certify that any relevant findings about the matching program from the agency IG or from GAO were adequately taken into account. The CPO must also certify that the matching activity addressed any identified problem in previous matching programs.

Two additional required certifications place considerable responsibility on the agency CPO. Both apply except where a statute mandates that a matching program occur. First, the CPO must express a judgment that the matching activity is financially justified based on relevant results of current or past matching programs. This too is a substitute for the existing requirement that the agency assess costs

and benefits of matching. Placing specific responsibility on an identified official rather than an unfocused and poorly defined requirement on an agency should produce a better result. The sharing of records always presents privacy concerns, and if the sharing is not financially justifiable, then the sharing should be reconsidered and ended when appropriate. The second certification calls on the CPO to express a judgment that the matching program is in the public interest. Record sharing through matching may have different purposes. While many of those purposes may relate to financial matters, there may be other reasons why sharing should not be allowed. The public interest standard here is broad and allows a CPO to weigh all relevant factors related to a matching program and express a judgment.

Paragraph (a)(3) imposes another administrative control on matching. It prevents a source agency from entering into a second or subsequent agreement unless the other agency involved certifies in writing that it complied with the provisions of previous agreements. In addition, the source agency must have no reason to believe that the certification is inaccurate. Each source agency can establish the content and form of a certification. These requirements are virtually identical to those found in subsection (q) of the Privacy Act.

Paragraph (a)(4) provides for the posting of a copy of each matching agreement together with the certification of the FPO on the source agency's website. A copy of the agreement also must go to OMB. The bill does not continue the requirement for congressional notification.

Paragraph (a)(5) provides that a matching agreement cannot be effective until posted on the agency website for 30 days.

Paragraph (a)(6) continues existing language from the Computer Matching and Privacy Protection Act of 1988.[238] One provision makes it clear that the USA FIPS Act does not authorize any matching program not otherwise authorized by law. The Act regulates matching, but it does not provide independent authority for matching. Another provision that was part of the 1988 Act makes it clear that the USA FIPS Act does not authorize disclosing records to anyone other than a government agency for a matching activity. Any authority for other disclosures must derive from another law.

2. Due Process Requirements

(b) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS. –

(1) TIME FOR NOTICE AND RESPONSE. – In order to protect an individual whose record is used in a matching program, no source agency or non-Federal agency using a record from a matching program may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to the individual, or take other adverse action against the individual, as a result of information produced by the matching program, until –

(A)(i) the source agency has independently verified the information; or

(ii) the Chief Privacy Officer of the source agency determines in accordance with guidance issued by the Director of the Office of Management and Budget that–

[238] Public Law 100-503, Act of Oct. 18, 1988, 102 Stat. 2514, 5 U.S.C. § 552a note. The language is in the Public Law but not in the text of the Privacy Act in U.S. Code. There are two other similar rules of construction not included in the USA FIPS Act. One addresses "the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies" and the other "the direct linking of computerized systems of records maintained by Federal agencies." Both provisions seem technologically outdated. Their omission does not reflect a change of policy.

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest the findings; and

(C) the expiration of –

(i) any time period established by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no the period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) BASIS FOR ADVERSE ACTION. – The independent verification referred to in paragraph (1)(A)(i) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of–

(A) the amount of any asset or income involved;

(B) whether the individual actually has or had access to the asset or income for the individual's own use; and

(C) the period or periods when the individual actually had the asset or income.

(3) HEALTH AND SAFETY EXCEPTION. – Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by the paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by the paragraph.

Subsection (b) contains the verification requirements for matching. These are largely unchanged, except that the responsibility that the Privacy Act assigns to Data Integrity Board is given to the agency CPO.

Paragraph (b)(3) is the same as current law. The reason for highlighting the health or safety exception here is the COVID-19 pandemic. An agency has broad authority to take appropriate action that might be otherwise prohibited in paragraph (b)(1) if public health or public safety may be adversely affected or significantly threatened by the notice period. That means that any matching activity that falls under the USA FIPS Act should not interfere with any appropriate public health activities responsive to the pandemic or any similar threat.

P. Miscellaneous (Section 16)

Section 16 is a collection of existing provisions, changed provisions, and new provisions about various aspects of the USA FIPS Act.

1. Waivers

(a) WAIVER. – A waiver of the rights under provided under section 7 and section 8 of this Act is against public policy and is void and unenforceable.

Subsection (a) provides that an individual's waiver of the rights under section 7 and section 8 of the Act is against public policy and is void and unenforceable.[239] These are the rights of access, the right to request an amendment, and the right to request a disclosure history. No federal agency can ask for or honor a waiver of these rights. This restriction on waiver of rights has nothing to do with, and does not affect, an individual's ability to waive their privacy rights in order to permit disclosure of that individual's records to a third person under the FOIA or otherwise.

2. Sale of PII

(b) SALE OF PERSONALLY IDENTIFIABLE INFORMAITON. – An individual's name; postal and electronic addresses; telephone numbers; and other personally identifiable information may not be sold or rented by an agency unless specifically authorized by statute. This provision shall not be construed to require the withholding of personally identifiable information otherwise permitted to be made public.

Subsection (b) continues an existing provision of the Privacy Act that prohibits an agency from selling or renting of mailing lists unless specifically authorized by law. The revised provision makes it clear that the prohibition extends to all other PII, not just addresses. Any allowable sale or rental must be specifically authorized by statute. As with the current provision, the prohibition does not interfere with the disclosure of PII otherwise permitted to be made public. Thus, this prohibition would not affect a statute that makes public ethics filings by government officials.

3. FOIA

(c) EFFECT OF OTHER LAWS. –
(1) FOIA EXEMPTIONS NOT APPLICABLE TO RIGHTS UNDER THIS ACT. – No agency shall rely on any exemption contained in section 552 of title 5, United States Code, to withhold from an individual any record that is otherwise accessible to the individual under the provisions of this Act.
(2) EXEMPTIONS UNDER THIS ACT NOT APPLICABLE TO FOIA. – No agency shall rely on any exemption in this Act to withhold from an individual any record that is otherwise accessible to the individual under the provisions of section 552 of title 5, United States Code.

Subsection (c) continues existing language in subsection (t) of the Privacy Act about the interplay between the FOIA and the USA FIPS Act. An agency cannot rely on a FOIA exemption to withhold a record that is otherwise accessible under the USA FIPS Act. Similarly, exemptions in the USA FIPS Act cannot be used to withhold from an individual any record that would otherwise be accessible to that individual under the FOIA. Both provisions came about when the Department of Justice began to

---

[239] Waiver has been an issue in FOIA cases involving criminal defendants. See generally, Department of Justice, Guide to the Freedom of Information Act, Procedural Requirements, text accompanying notes 93-95 (2019), https://www.justice.gov/oip/page/file/1199421/download. In some criminal plea agreements, defendants waive their rights to file FOIA requests. In *Price v. DOJ*, 865 F.3d 676, 683 (D.C. Cir. 2017), https://www.cadc.uscourts.gov/internet/opinions.nsf/0/BC2ECD2C67FCA691852581720053BDCF/$file/15-5314-1687329.pdf, the court found that a plea agreement that attempts to waive a right conferred by a federal statute is, like any other contract, "unenforceable if the interest in its enforcement is outweighed [under] the circumstances by a public policy harmed by enforcement." The policy established here is that the individual rights under the USA FIPS Act cannot be waived as a matter of public policy.

argue in the early 1980s that the Privacy Act or the FOIA authorized withholding of records from individuals for which there was no justification.

4. Rights of Parents and Guardians

(d) RIGHTS OF PARENTS AND GUARDIANS. – A parent, guardian, other person acting in loco parentis, or person with a valid power of attorney who under applicable law has authority to act on behalf of an individual may act on behalf of the individual under this Act.

Subsection (d) continues and expands upon an existing provision in subsection (h) of the Privacy Act regarding rights of legal guardians. First, the language is a bit more expansive in describing who can act on behalf of another individual, including now specifying that a person with a valid power of attorney may also act on behalf of the individual under the USA FIPS Act. The bill drops language in the Privacy Act requiring an individual to be first declared to be incompetent by a court. Instead, the bill borrows language from HIPAA about *authority to act on behalf of an individual*.[240] Requiring formal proceedings before an individual can act on behalf of a spouse, adult child, or parent in cases involving dementia, impairment, or other circumstances is too restrictive. Agencies will have more leeway to act appropriately and compassionately here in accordance with any applicable law.

5. Reports to Congress

(e) REPORT TO CONGRESS. – Each agency that proposes to establish or make a change in an agency activity affecting privacy that significantly limits or otherwise alters the rights and opportunities available to individuals under this Act, or that adds or significantly modifies an agency designated disclosure shall provide adequate advance notice to appropriate Committees of Congress and to the Office of Management and Budget.

Subsection (e) is comparable to subsection (r) of the Privacy Act, providing for reports on new or changed A3Ps or ADDs to appropriate House and Senate committees and to OMB.

6. Website

(f) WEBSITE. – Each agency shall maintain a privacy website, with appropriate search, indexing, and finding aids, that allows for the full search and downloading of text maintained on the website. The website shall include –

(1) the notice for each current agency activity affecting privacy and any personally identifiable information processing diagram prepared in accordance with section 9(d) of this Act;

(2) a complete history of all changes made in the past ten years to the notice of each agency activity affecting privacy, including the full text of each prior published notice, an identification of all changes, and the date on which each change took effect;

(3) a complete list of all Federal Register notices, including all amendments, for each agency activity affecting privacy, together with an electronic or digital link to each notice;

(4) the text of all system of records notices and amendments published under the Privacy Act of 1974 for the ten-year period before completion of the agency transition to compliance with this Act;

---

[240] 45 C.F.R. § 164.502(g).

(5) information about, and to the extent practicable, a copy of each privacy impact assessment report completed in the past twenty-years or currently being conducted;

(6) other information determined by the head of the agency or by the Chief Privacy Officer to be helpful to the public in understanding agency privacy activities, the provisions of this Act, and the exercise of privacy rights granted by this Act to individuals; and

(7) information about the agency's plans for transition from compliance with the Privacy Act of 1974 to compliance with this Act.

Subsection (f) directs each agency to establish a privacy website and describes required content. The website must allow for the full search and downloading of all text maintained on the privacy website. The search capability must be able to limit the search to the contents of the privacy website separately from material maintained by the agency on other websites.

The website must include the current notice for each A3P. It must include any personally identifiable information processing diagram prepared in accordance with section (9)(d) of the Act. The website must include a complete history of all changes made in the past ten years to each A3P, including the full text of each prior published notice, an identification of all changes, and the date on which the changes became effective. The goal is to establish a one-stop shop so that individuals can see how an agency organized its records in the past and which description applied at what time. Another element is a list of all Federal Register notices for each A3P. These requirements apply after the effective date of the USA FIPS Act.

Each agency must also provide the text of all system of records notices and amendments published under the Privacy Act for the ten-year period prior to its transition to the USA FIPS Act. An agency may, but is not required to, tie previous systems of record notices to new A3Ps. Finding and cross-reference aids would be useful to the agency and the public, but the bill does not direct their creation.

The website must include information about each past PIA and about each PIA currently being conducted. The website must provide a copy of each PIA to the extent practicable. The practicability standard here recognizes that there may be elements of a PIA not suitable for public disclosure.

The website must include other information determined by the head of the agency or by the Chief Privacy Officer to be helpful to the public in understanding agency privacy activities, the provisions of the USA FIPS Act, and the exercise of privacy rights granted by this Act to individuals. Under this authority, it would be appropriate for an agency to include a form or method for an individual to make a request under the Act for access to or amendment of records.

Finally, the agency must post information about its plans for the transition from compliance with the Privacy Act to compliance with the USA FIPS Act.

7. Statute or Treaty

(g) STATUTE OR TREATY. – The failure of an agency to identify a statute or treaty requiring or specifically authorizing disclosure of a record in any notice or publication under this Act shall not overcome any requirement or authorization to disclose the record as provided in the statute or treaty.

Subsection (g) addresses the requirement in section (6)(f)(2)(D) that an agency make a good faith effort to specify as an agency designated disclosure each statute or treaty that requires or specifically

authorizes disclosure of personally identifiable information. Subsection (g) makes it clear that an agency's failure in a published notice to identify a statute or treaty requiring or specifically authorizing disclosure of a record does not overcome the requirement or authorization to disclose a record as provided in the statute or treaty. It is likely that agencies will not always be able to find all of these provisions or to keep notices up-to-date. Substantive authority to disclose in another law remains valid. An agency should, upon finding an omission, promptly update its publications. The authority here to disclose notwithstanding a notice failure applies only to disclosures required by or specifically authorized by treaty. It does not extend to a disclosure that an agency must otherwise authorize by publishing an ADD.

Q. Agency Rules (Section 17)

(a) AGENCY RULES. – In order to carry out the provisions of this Act, each agency that maintains an agency activity affecting privacy shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of title 5, United States Code, that shall –

(1) establish procedures whereby an individual can be notified in response to the individual's request if any agency activity affecting privacy identified by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for authenticating the identity of a data subject who requests a record or information pertaining to the data subject before the agency shall make the record or information available to the data subject;

(3) establish procedures for the disclosure to a data subject upon request the data subject's record;

(4) establish procedures for reviewing a request from a data subject for amendment of any record or information, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for a data subject to be able to exercise fully the data subject's rights under this Act;

(5) describe any limits that apply to the exercise of rights under this Act as a result of exemptions and including the name of any agency activity affecting privacy to which exemptions apply;

(6) establish fees to be charged, if any, to a data subject for making a copy of records requested under this Act, excluding the first 1000 pages of records provided on paper, any record provided in electronic form or format, and the cost of search for and review of the records; and

(7) establish rules of conduct for persons involved in the design, development, conduct, or maintenance of any agency activity affecting privacy, or in processing any personally identifiable information, and instruct each person about the rules and the requirements of this Act and the penalties for noncompliance.

(b) COMPILATION. – The Office of the Federal Register shall biennially compile and publish on a public website available without charge the rules promulgated under this Act and agency notices published under section 5 of this Act, together with appropriate search, indexing, and finding aids.

Section 17 brings together with little change existing provisions from subsection (e)(9) and subsection (f) of the Privacy Act. Paragraph (a)(6) places limits on fees for a copy of records. The first thousand pages and any record provided in electronic form or format are free. Costs for records beyond the amounts established here should be charged at a cost not to exceed that allowed under the FOIA. As provided under the Privacy Act, an agency will not be allowed to charge for search and review of records. Subsection (b) is similar to an existing requirement, except that the Federal Register cannot

charge for use of its privacy website, and it must provide the public with search, indexing, and finding aids. This just updates the existing provision, which originated decades before the Internet. The Federal Register already provides useful Privacy Act pages, although improvements to those pages are possible.[241]

As noted elsewhere, the existing provision in paragraph (f)(3) providing the option for a special procedure for medical records does not appear in the USA FIPS Act.

R. Civil Remedies. (Section 18)

(a) REMEDY. – A data subject may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this section, whenever any agency –

(1) fails to comply with the data subject's request under section 7(a) or section 8(b)(2) of this Act;

(2) decides after review not to amend the data subject's record in accordance with the data subject's request under section 7(b) of this Act, or fails to make the review in conformity with that section;

(3) fails to process any record concerning the data subject with sufficient accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, benefits, privileges, or status, of the data subject that may be made on the basis of the record, and consequently a determination is made which is adverse to the data subject; or

(4) fails to comply with any other provision of this Act, or any rule promulgated thereunder, in a way that has an adverse effect, including mental or emotional distress, on the data subject.

(b) APPEAL.

(1) INJUNCTION TO PROVIDE RECORDS. –In any suit brought with respect to a failure described in subsection (a)(1), the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld. The court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in section 12 of this Act. The burden is on the agency to sustain its action.

(2) INJUNCTION TO AMEND RECORDS. – In any suit brought with respect to a decision or failure described in subsection (a)(2), the court may order the agency to amend the data subject's record in accordance with the data subject's request or in any other way as the court may direct. The court shall determine the matter de novo.

(3) DAMAGES AND COSTS. – In any suit brought with respect to a decision or failure described in subsection (a)(3) or (a)(4) in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the data subject for –

(A) provable damages, including mental or emotional distress, sustained by the data subject as a result of the refusal or failure or $1000, whichever is greater, but in any class action, the court may reduce the damage award if the total damages are excessive or otherwise unwarranted; and

(B) the costs of the action together with reasonable attorney fees and other litigation costs as determined by the court;

---

[241] See Privacy Act Issuances, 1995 to Present, https://www.govinfo.gov/help/pai, and Privacy Act Issuances, https://www.govinfo.gov/app/collection/PAI.

(4) VENUE AND STATUTE OF LIMITATIONS. – An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or in which the complainant has a principal place of business, or in which the agency headquarters are located, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that if an agency materially and willfully misrepresented any information required under this Act to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this Act, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

The civil remedies in the USA FIPS Act are substantially similar to those in the Privacy Act. The most significant substantive change is in the damages provision. There are two important differences. First, the standard for damages is *provable damages, including mental or emotional distress*. The use of *provable damages* moves away from the existing terminology and the tortured history of its interpretation. The overall effect is to overturn the holdings in *Doe v. Chao*[242] and *FAA v. Cooper*[243] so that a successful plaintiff can recover for any provable damages and not just pecuniary or out-of-pocket losses. Further, a plaintiff who cannot show any damages is entitled to receive $1000. Proof of damages is not a requirement to receive the $1000 minimum.

Second, the damages provision gives court discretion to reduce damage awards in class actions if the total damages are excessive or otherwise unwarranted. This is a deliberately broad standard. In other areas of privacy law or consumer law, the possibility of large awards of damages for minor or technical violations of law can result in a finding against deserving plaintiffs because of fixed damage formulas that produce large and mandatory damage awards that are disproportionate to the violation. The most important result in a case under section 18 is a determination whether an agency violated the law. The goal here is to make sure that a court can reach that finding when appropriate without being forced into an unreasonably large damage award in a class action lawsuit. For example, in the event of a breach of all data subject records at the Social Security Administration where there are no provable damages, the award of $1000 to each plaintiff would be a judgment against the United States in the tens of billions of dollars. In that case, a court might reduce the award to token damages and make a cy pres award to suitable public interest groups of a fraction of the theoretical entitlement.

Nothing in the civil remedies section overturns the "well settled" understanding that injunctive relief is only available in cases involving access and amendment.[244] The Privacy Act did not give the courts the ability to enjoin government programs for technical or other violations of the Act. The draft bill continues that policy. Further, nothing here changes the policy in the Privacy Act of 1974 that the civil remedies provision does not create an opportunity to collaterally attack information or decisions for which adequate judicial review is otherwise available.[245] In too many Privacy Act cases, plaintiffs try to

---

[242] *Doe v. Chao*, 540 U.S. 614 (2004).

[243] *Federal Aviation Administration v. Cooper*, 566 U.S. 284 (2012).

[244] Department of Justice, Overview of the Privacy Act of 1974 at 245 (2015 edition).

[245] Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Federal Register 28948-79, at 28969 (July 9, 1975) ("For example, these provisions were not designed to afford an individual an alternate forum in which he can challenge the basis for a criminal conviction or an asserted tax deficiency.").

use the Act to reopen matters for which other remedies exist and in which the plaintiffs lost. These plaintiffs typically lose the Privacy Act cases too, as well they should.

S. Administrative Remedy (Section 19)

Section 19 establishes a new remedy that any person can use to ask an agency to comply with the USA FIPS Act. This remedy is needed because it can be nearly impossible to challenge many illegal agency actions under the Privacy Act. An individual harmed by an agency failure to comply has a remedy, but that leaves no opportunity to challenge many agency actions. For example, an agency issues a system of records notice with an illegally broad routine use. Unless an individual can show harm resulting from an actual improper disclosure of their record under that routine use, there may be no way for anyone to object. For some exempt systems of records, for example, it may be impossible for an individual to even learn that the agency disclosed their record at all. Some systems may be exempt from the requirement to share disclosure history (accounting) records with the individual.[246] Even when disclosure history records are available, it could take a long time before any individual with the knowledge and wherewithal to use the civil remedy learns of a disclosure under an illegal routine use. That means that an agency can operate for years or decades disclosing records under an illegal routine use.

The lack of a broad administrative remedy and the absence of the ability to take an agency to court explains in part some aspects of agency noncompliance of the Privacy Act. There is no effective oversight or remedy by some affected individuals or by public interest groups. That means it is possible for an agency to fashion its own method of implementing the Act and proceed almost in any way that it chooses, free from any realistic possibility of public oversight. Current oversight mechanisms, including review of agency Privacy Act publications by OMB and by the Congress, are inadequate to the purpose. An effective way for public challenge of compliance with the USA FIPS Act is essential for the success of the Act.

The administrative complaint process may not see significant use in the first few years under the new law. Agencies must publish A3P descriptions under notice-and-comment rulemaking procedures. Those who are unhappy about how an agency implements the new law can use the notice and comment process to raise most concerns. For agencies that receive comments and address them fairly, there may be few if any administrative complaints for some time.

(a) COMPLAINT. –

(1) Any person may file with the Chief Privacy Officer of the agency a complaint setting forth specific facts alleging that an agency failed to comply in a material way with this Act, including any provision regulating –

(A) publication of a timely and accurate description of an agency activity affecting privacy;

(B) a properly defined and adopted agency defined disclosure;

(C) a meaningful and timely privacy impact assessment process;

(D) matching programs; or

(E) any other action specified in this Act.

[246] Agencies can exempt some systems from the civil remedies altogether, although the courts tend to read that exemption narrowly and look for ways to allow at least some civil actions.

(3) The Chief Privacy Officer of the agency shall –

(A) acknowledge receipt of a complaint under this subsection in writing within ten days;

(B) within 90 days, either (i) reject a complaint that lacks sufficient specificity to adequately identify or support the allegations in the complaint that otherwise fails to meet the requirements of this section and promptly notify the complainant of the right to appeal under this section, or (ii) if any allegations in the complaint are found to be meritorious, promptly inform the complainant of that decision and undertake reasonable steps to correct any identified deficiencies.

1. Complaint

The new administrative remedy has similarities to the process under the Freedom of Information Act. Under the FOIA, any person can request records from an agency. If that requester is not satisfied with the response (whether substantive or procedural), the requester can appeal to federal court.

Under section 19, any person can file a complaint with the CPO of an agency alleging based on specific facts that an agency failed to comply in a material way with the Act. Paragraphs (1) (A) through (E) provide examples of the types of agency failures that may give rise to a complaint, with (E) providing a catch-all for any failure not expressly specified otherwise.

Noteworthy elements for a complaint are the requirements that the complaint provide *specific facts* about the agency failure and that the failure to comply be *material*. A CPO can reject a complaint that lacks sufficient specificity to adequately identify the problem, support the allegations in the complaint, or explain the materiality of the failure. Thus, a CPO may reject a complaint that alleges that the agency's ADDs are out-of-date if the complaint does not identify the ADDs in question or explain in a brief way why they are deficient. However, the burden on a complainant is limited. No complainant is obliged to file a lengthy legal brief or to make extensive factual arguments. A valid complaint could simply allege, for example, that the agency did not revise its A3P description for an agency program that significantly altered the way the agency processes PII. The materiality of some failures, such as an improper description, may be apparent. CPOs should not rely on overly technical complaint standards or reject complaints too quickly if there is a problem that can be identified and addressed, even if the problem is minor.

This broad standard gives the CPO leeway to reject complaints that are too vague, significantly incomplete or repetitive. It is possible that complaints will identify small matters that the CPO can readily correct. Trivial complaints (e.g., typographical errors in a description that do not interfere with understanding) might be rejected.

Paragraph (a)(3) sets out the process. The agency CPO must acknowledge a complaint within ten days of receipt. The bill is silent on the form of the written response, and the CPO can use postal mail or electronic mail depending on the method used to file the complaint or a method requested by the complainant. The CPO has 90 days to make a substantive response. The CPO can reject a complaint for lack of sufficient specificity to identify or support the allegations or for lack of merit. If the complaint is found meritorious, the CPO must promptly notify the complainant and must undertake reasonable steps to correct any identified deficiencies. A complaint may, of course, be accepted in part and rejected in part.

The CPO must determine what constitutes reasonable steps as a response to each meritorious complaint. Republication of a corrected A3P notice might be a reasonable step. Correction of material failures in an agency PIA process might reasonably require revision of the process or the report. The timing of the CPO's response to a meritorious complaint should be judged by a reasonableness standard as well. Some errors may be readily corrected, but some may take months to complete. If a PIA process overlooked material considerations, a CPO may need to redo part of the process and the report, but it may take considerable time and effort to do so. Other priorities and available resources may be relevant to the scheduling of an unplanned major activity identified in a complaint. However, an indefinite postponement of a substantive correction of a failure identified in a meritorious complaint would not be reasonable.

Nothing in the administrative remedy requires an agency that receives a meritorious complaint to stop program operations, sharing of PII, or other lawful activities pending correction of failures to comply with the USA FIPS Act. No damages are available under the section 19 administrative remedy. A data subject can only seek damages under the civil remedies in section18.

2. Judicial Review

(b) JUDICIAL REVIEW. –
(1) ACTIONS AUTHORIZED. – A complainant whose complaint under this section –
(A) was denied in whole or in part by the agency;
(B) was determined to be meritorious, but on which the agency unreasonably delayed corrective actions; or
(C) did not receive a substantive response from the agency within three months after filing the complaint –
may bring a civil action against the agency to obtain judicial review pursuant to sections 701 through 705 of title 5, United States Code, and the district courts of the United States shall have jurisdiction in the matter.
(2) VENUE. – An action under this section may be brought in the district court of the United States in the district in which the complainant resides, or has a principal place of business, or in which the agency headquarters are located, or in the District of Columbia, without regard to the amount in controversy.
(3) ORDERS. – The court may order the agency to correct any material failure to comply with this Act.
(4) COSTS. –The court may assess against the United States the costs of the action together with reasonable attorney fees and other litigation costs as determined by the court in any case under this section in which the complainant has substantially prevailed.

Subsection (b) provides for judicial review of the CPO's treatment of a complaint. Judicial review is the same as for any other administrative matter under the terms of the Administrative Procedure Act. There are three specific grounds for judicial review: an agency denied a complaint in whole or in part by the agency; an agency unreasonably delayed corrective actions identified by a meritorious complaint; or the agency did not respond substantively to the complaint within 90 days.

If a court finds that the agency failed to correct any material failure to comply with the USA FIPS Act, it may order the agency to correct the failure. This open-ended direction gives the court wide latitude

to fashion an appropriate order, taking into account the nature of the agency's failure and the time needed to correct the failure.

T. Effective Date and Transition (Section 20)

Most agencies will find transitioning from compliance with the Privacy Act to compliance with the USA FIPS Act somewhat challenging. Much of what is in the USA FIPS Act is evolutionary, but some parts are new. Changes in information technology since 1974 have been revolutionary, and some of the changes allow agencies to do a better job of compliance with privacy requirements. Agencies have considerable discretion in establishing the scope of each A3P, and it is likely that many agencies will restructure their existing systems of records in ways that require rethinking how administrative controls will work and which agency designated disclosures are appropriate. Some agencies may find that existing approaches still work under a new law. Regardless, a new law is an opportunity to reexamine decisions that, in some instances, agencies made first in 1975 and never reexamined.

Perhaps the most significant administrative requirement is the need to do notice-and-comment rulemaking when publishing A3P descriptions. This initial obligation will place an additional modest burden, and the republication of all privacy notices will also be a modest burden. Once an agency completes the transition, compliance with the USA FIPS Act should not be more complicated or expensive than existing law.

The transition provision gives agencies both considerable discretion in deciding on a new structure for defining its PII processing activities, and a long time to carry out the transition. The transition period is five years, with the possibility of a two-year extension. One thing I learned in establishing legislative deadlines for agency actions is that everything takes longer than anyone expected.

It may be unlikely that more than a few agencies will need five years to complete the transition. However, an agency like the Department of Defense and perhaps a few other large agencies with many systems of records may need a long time to complete the work. OMB has the authority to grant a two-year extension.

1. Effective Date

(a). EFFECTIVE DATE. – This Act shall take effect ten days after the date of enactment. Agencies shall comply with this Act as provided in this section.

The law is effective ten days after the date of enactment. The date on which agency must comply with the USA FIPS Act is not the date of enactment, but the date specified in other parts of section 20. The effective date marks the starting point for the law's timed requirements.

2. Transition

(b) TRANSITION. – Within one year after the effective date of this Act, each agency subject to the Privacy Act of 1974 shall prepare a transition plan for changing its privacy compliance activities from section 552a of title 5, United States Code, to this Act. Each agency shall send a copy of its plan to the Director of the Office of Management and Budget and shall post a copy of its plan on the agency's privacy website.

Each agency must develop a formal plan for the transition from the Privacy Act to the USA FIPS Act and send the plan to OMB. For smaller agencies, the plan might be short and simple. For agency with dozens, hundreds, or thousands of systems of records, developing a plan will require significant effort. Each agency must post its plan on its privacy website, and the website will provide a useful way to keep the public informed about the progress of the agency's transition.

3. Transition Plan

(c) TRANSITION PLAN. – The transition plan –

(1) shall establish a date when all components of the agency will comply with this Act, not to exceed five years from the date of enactment;

(2) shall provide for the promulgation of agency rules required by this Act before any part of the agency completes the transition;

(3) shall provide for publication of a notice disclosing the date of transition in the Federal Register at least 30 days before the date when all or part of the agency completes the transition to this Act;

(4) shall, not less frequently than every six months until the transition for the entire agency is complete, provide for public notice of the progress of the agency's transition on the agency's privacy website;

(5) may provide different transition dates for different agency components.

Subsection (c) sets out the required content of the transition plan. Each plan must have a target date for completion, provide for the promulgation of required agency rules, and provide public notice in the Federal Register of the date of transition. An agency must keep the public notified of transition progress on its website not less than every six months. The requirement to publish agency rules should not present major difficulties because the rules will be substantially similar to existing Privacy Act rules. When reissuing those rules, agencies that have not revisited their Privacy Act rules can bring the rules up to date.

Finally, an important feature of the transition is that an agency can provide different transition dates for different agency components. This means that an agency's transition does not have to occur at once. An agency like the Department of Defense with so many separate components will have the ability to transition over time. Other agencies may also welcome the ability to transition piecemeal and not to manage a single event for all components.

4. PIA During Transition

(d) PRIVACY IMPACT ASSESSMENT DURING TRANSITION. – (1) An agency may choose not conduct a privacy impact assessment process as provided in section 11 before it first establishes an agency activity affecting privacy during the transition to compliance with this Act if the agency determines that –

(A) a recent privacy impact assessment substantially accomplished the purposes set out in section (11)(a) for the agency activity affecting privacy; or

(B) the agency activity affecting privacy only requires a limited privacy impact assessment and the activity is comparable to an activity covered by a privacy impact assessment conducted during the five years before the initial establishment of the activity.

(2) In determining priorities and allocating resources for privacy impact assessment processes during the transition, the agency shall give priority to new agency activities affecting privacy, to

activities that are likely involve greater risk to the agency or to data subjects, and to any novel or innovative applications of technology.

Subsection (d) provides a special rule for the PIA process during the transition. It is unlikely that an agency will be able to go through a PIA process – and certainly not a thorough process – for each A3P it establishes. Agencies are unlikely to have the time or the resources to conduct all possible PIA processes. An agency has discretion to not conduct a PIA process if it conducted a recent one (under the E-Government Act standard or otherwise) that substantially accomplished the purposes set out in section 11. An agency may also choose not to conduct a limited PIA process if conducted something comparable in the last five years. The standards here for determining whether a previous PIA process will serve the purpose are different. For a thorough PIA process, the previous PIA should be substantially similar. For a limited PIA process, the previous PIA need only be comparable, a weaker standard.

Paragraph (d)(2) recognizes that an agency may not be able to conduct all possible PIA processes. It directs agencies to give priority to new activities, to activities that involve greater risk to the agency or to data subjects, and to any novel or innovative applications of technology. Over time, agencies will eventually be able to conduct PIA processes for more A3Ps that require them.

5. Termination

(e) TERMINATION. – An agency or agency component that completes the transition from the section 552a of title 5, United States Code, to this Act shall terminate compliance with section 552a of title 5, United States Code, on the transition date for the agency or agency component.

Subsection (e) establishes a termination date for compliance with the Privacy Act of 1974. That date is the transition date established for the agency or component. Thus, until a government-wide transition occurs, some agencies and some parts of agencies will be subject to different privacy laws. Given that the laws have many similarities, this should not present any significant problems.

6. OMB

(f) OFFICE OF MANAGEMENT AND BUDGET. –

(1) The Director of the Office of Management and Budget shall issue guidance to agencies regarding the transition from section 552a of title 5, United States Code, to this Act.

(2) Upon the request of an agency, the Director of the Office of Management and Budget may allow the agency to amend its transition plan and to take additional time to complete the transition. No extension may be granted beyond seven years from the date of enactment of this Act.

(3) Until the transition is complete for all agencies, the Director of the Office of Management and Budget shall report annually to the Congress and to the public on the government's progress in transitioning to compliance with this Act.

Subsection (f) sets out the role of OMB in the transition. First, OMB must issue transition guidance to agencies. This will help ensure that agencies meet all appropriate requirements. Second, OMB has the authority to allow agencies to amend their transitions plans, including the ability to give agencies up to an additional two years to complete the transition. Finally, OMB must report annually to the Congress and the public on transition progress.

7. Litigation

(g) LITIGATION. – Any litigation initiated under the section 552a of title 5, United States Code, shall be unaffected by this Act and shall continue under the provisions of the section 552a of title 5, United States Code, notwithstanding whether the agency completed its transition to this Act.

Subsection (g) preserves the status of any Privacy Act litigation initiated before an agency completed its transition to the USA FIPS Act.

U. Other Matters

1. CFPB

Subsection (w) of the Privacy Act provides:

> Applicability to Bureau of Consumer Financial Protection. – Except as provided in the Consumer Financial Protection Act of 2010, this section shall apply with respect to the Bureau of Consumer Financial Protection.

I have been unable to find any explanation for this provision or any evidence that it has any actual effect on the operations of the Consumer Finance Protection Bureau. There is a reference to privacy in the CFPB's statute that says:

> (8) Privacy considerations
>
> In collecting information from any person, publicly releasing information held by the Bureau, or requiring covered persons to publicly report information, the Bureau shall take steps to ensure that proprietary, personal, or confidential consumer information that is protected from public disclosure under section 552(b) or 552a of title 5 or any other provision of law, is not made public under this title.[247]

This language essentially directs the Bureau to comply with the Privacy Act.

As a result, I did not include subsection (w) in the USA FIPS Act because it appears to be unnecessary.

2. Codification

As presently drafted, the USA FIPS Act is a freestanding law. It would be appropriate, however, for the Act to be codified in U.S. Code. There are two obvious choices. The Privacy Act of 1974 is part of title 5 in the Administrative Procedure chapter. Given the current numbering scheme there, there is no particularly convenient place there for a new subchapter. It is always possible to add something in between what is there by adding letters at the end of section numbers. The codification of the Privacy Act as title 5, U.S.C. § 552a is mostly a consequence of the law emerging from the same House committee that produced the Freedom of Information Act, which is 5 U.S.C. § 552.

---

[247] 12 U.S.C. § 5512(c)(8), https://www.law.cornell.edu/uscode/text/12/5512.

A better alternative may be title 44, chapter 31, which covers records management by federal agencies. Privacy legislation is largely a records management matter, and other relevant records management provisions are in title 44 already. There is "room" in chapter 31 for adding a new law with 20 sections.

In the end, I did not address the codification issue in the bill itself. Codifying a law in an existing positive title makes the drafting procedurally more cumbersome. It is better to allow readers of the draft to focus on the content of the bill rather than the drafting details. A choice about codification can be made at a later date.

3. Social Security Numbers

Section 7 of Public Law 93-579 provided that:

> (a) (1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.
> (2) the provisions of paragraph (1) of this subsection shall not apply with respect to –
> (A) any disclosure which is required by Federal statute, or
> (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.
> (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.[248]

This limit on the use of Social Security Numbers is distinctive because it applies to state and local government agencies as well as federal agencies. In part because this provision was never codified, and in part because it applies to all levels of government, the limit has been ignored at times, especially at the state and local levels. Additionally, later legislation exempted some state agencies from compliance in the administration of tax, public assistance, drivers licenses, and motor vehicle registration.[249] Still, the law applies elsewhere, and there has been litigation over use of SSN over the years. Judicial opinions reflect a wide range of views on the applicability and enforceability of Section 7.[250]

In the end, I decided to leave section 7 alone. While it might be useful to include it in a codified law, the provision presents several problems. First, it would be the only provision of the USA FIPS Act to apply to state and local agencies. Second, the provision has no clear enforcement provision, and adding one might create new policy and political problems. Third, clarifying some of the language of section 7 might be appropriate, but it could upset some understandings of the provision and contribute to political problems. Fourth, while section 7 was innovative when passed, there are larger

---

[248] Pub. L. 93–579, § 7, Dec. 31, 1974, 88 Stat. 1909, https://www.law.cornell.edu/uscode/text/5/552a note.

[249] 42 U.S.C. § 405(c)(2)(C), https://www.law.cornell.edu/uscode/text/42/405. Other exemptions exist as well.

[250] See Department of Justice, Privacy Act Overview 307-312 (2015), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

problems with the collection of identification numbers than can reasonably be addressed in the USA FIPS Act. I flag the issue here for anyone who cares to tackle it in the future.

*****

Version History

Version 2.0. First Public Version, March 22, 2021
Version 2.01. Corrected typos and format matters, April 19, 2021.

Appendix 1. Text of the Proposed United States Agency Fair Information Practices Act

Version 2.3

Sec. 1. Short Title.

This Act may be cited as the "United States Agency Fair Information Practices Act (USA FIPS Act)".

Sec. 2. Findings and Purposes

(a) FINDINGS. – The Congress finds that –

(1) the right to privacy is a personal and fundamental right protected by the Constitution of the United States;

(2) the privacy of an individual is directly affected by the processing of personal information by Federal agencies;

(3) the increasing use of sophisticated information technology, data mining, artificial intelligence, and profiling of individuals and households greatly magnifies the harm to individual privacy that can occur from any unjustified, unnecessary, or careless processing of personal information;

(4) the opportunities for an individual to secure employment, insurance, and credit, to participate in social, political and economic marketplaces, and to achieve due process and other legal protections are endangered by any unjustified, unnecessary, or careless processing of personal information;

(5) in order to protect the privacy of individuals identified in information systems processed by Federal agencies, it is necessary and proper for the Congress to regulate the processing of personal information by the agencies;

(6) it is appropriate and important for Federal agencies to inform the public about the nature of agency personal information processing activities and for agencies to maintain accurate and current descriptions and records of those activities;

(7) reasonable implementation of the following principles of Fair Information Practices by Federal agencies will provide protections for individual privacy while allowing the Federal agencies to carry out their missions in an effective and efficient manner:

(A) the Principle of Collection Limitation provides that there should be limits to the collection of personally identifiable information, that the information should be collected by lawful and fair means, and that the information should be collected, where appropriate, with the knowledge or consent of the data subject;

(B) the Principle of Data Quality provides that personally identifiable information should be relevant to the purposes for which they are to be processed, and to the extent necessary for those purposes should be accurate, complete, and timely;

(C) the Principle of Purpose Specification provides that there must be limits to the processing of personally identifiable information and that the information should be processed only for the purposes specified at the time of collection and for compatible purposes;

(D) the Principle of Disclosure Limitation provides that personally identifiable information should not be disclosed, except as provided under the purpose specification principle, without the consent of the data subject or other legal authority;

(E) the Principle of Security provides that personally identifiable information should be protected by reasonable security safeguards against risks including loss, unauthorized access, destruction, use, modification, and disclosure;
(F) the Principle of Openness provides that the existence of record-keeping systems containing personally identifiable information be publicly known, along with a description of the record keeper, main purposes, uses, disclosures, policies, and practices for processing the information;
(G) the Principle of Individual Participation provides that individuals should have a right to see personally identifiable information about themselves and to seek amendment or removal of information that is not timely, accurate, relevant, or complete; and
(H) the Principle of Accountability provides that a record keeper should be accountable for complying with fair information practices.

(b) PURPOSE. – The purposes of this Act are to provide safeguards for the personal privacy of individuals by requiring Federal agencies, except as otherwise provided by law –
(1) to permit individuals to know how agencies process personally identifiable information;
(2) to restrict the use and disclosure of personally identifiable information to lawful, defined, and disclosed purposes;
(3) to permit data subjects to gain access to personally identifiable information pertaining to themselves in Federal agency records, to have a copy of the records, and to ask for amendment to the records;
(4) to process any record in a manner that assures that –
(A) the processing is for a necessary and lawful purpose;
(B) the personally identifiable information in the record is current and accurate for its intended use; and
(C) the processing provides adequate safeguards to prevent misuse of the information;
(5) to be subject to civil suit for any damages which occur as a result of willful or intentional action that violates any individual's rights under this Act; and
(6) to allow any person who believes that a Federal agency is not complying with this Act to ask the agency to bring its conduct into compliance.

Sec. 3. Definitions.

In this Act:

- (1) INDIVIDUAL. –The term "individual" means a living individual and includes an individual acting as a sole proprietor.

(2) DATA SUBJECT. –The term "data subject" means the individual who is the principal subject of a record.

(3) PERSONALLY IDENTIFIABLE INFORMATION. – The term "personally identifiable information" means information about an identified or identifiable individual, including information about location, housing, education, finances, health, employment, criminal history, military service, taxation, agency program participation, Internet usage history, or any other personal activity or characteristic, and that contains any of the following data:
(A) a name;

(B) a home address, post office box, private mail box, or other physical or postal address;
(C) an e-mail address;
(D) a telephone number or the letters and numbers of a vehicle license plate;
(E) a Social Security Number; passport number; credit or debit card number; account, license, or employee number; or other identifying number assigned to an individual;
(F) date of birth;
(G) an Internet Protocol address or any comparable successor address;
(H) any other data that permits the physical or online contacting of a specific individual;
(I) a photograph, fingerprint, genetic, or other biometric identifier;
(J) information that identifies an individual's electronic device, including an international mobile equipment identity number, media access control address, contactless chip identifier, or any information that an agency Web site or online service collects online through a computer or from the individual, individual's cell phone, or other electronic device; or
(K) other information concerning an individual processed in combination with an identifier described in subparagraphs (A) through (J).

(4) AGENCY ACTIVITY AFFECTING PRIVACY. –The term "agency activity affecting privacy" means any agency function, program, or conduct that involves the processing of a record about an individual.

(5) RECORD. – The term "record" means any personally identifiable information processed by or for an agency as part of an agency activity affecting privacy.

(6) USE. –The term "use" means, with respect to a record, the employment, application, utilization, examination, sharing, or transfer of the record within the agency that processes the record.

(7) DISCLOSURE. –The term "disclosure" means, with respect to a record, the release, transfer, provision of access to, or divulging in any other manner of the record outside the agency that processes the record.

(8) PROCESSING. –The term "processing" or "processed" means, an activity with respect to a record, including the creation, collection, use, disclosure, maintenance, storage, examination, analysis, encryption, decryption, deidentification, reidentification, erasure, or destruction of the record.

(9) AGENCY DESIGNATED DISCLOSURE. – The term "agency designated disclosure" means a disclosure by an agency of a record from an agency activity affecting privacy that is –
(A) required or specifically authorized by Federal statute or treaty;
(B) appropriate to carry out the function of the agency activity affecting privacy from which the disclosure is made and for which the record was collected; or
(C) in support of another specified Federal activity or other specified activity for which the agency can appropriately disclose a record and the disclosure is not inconsistent with the purpose for which the record was collected.

(10) AGENCY. –The term "agency" means an agency as defined in section 552(f) of title 5, United States Code, and the Government Accountability Office, the Library of Congress, the Administrative Office of the United States Courts, the Government Printing Office, and the Smithsonian Institution.

(11) CLASSIFIED INFORMATION. – The term "classified information" means any information (1) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy; and (2) in fact properly classified pursuant to the Executive order.

(12) MATCHING PROGRAM. – The term "matching program" –

(A) means any automated comparison or other activity that involves the disclosure of –

(i) records processed in two or more two agency activities affecting privacy or from an agency activity affecting privacy with non-Federal agency records for the purpose of –

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under Federal benefit programs, or

(ii) Federal personnel or payroll records from two or more agency activities affecting privacy or from an agency activity affecting privacy with non-Federal agency records; but

(B) does not include –

(i) matches performed to support any research, statistical, or other activity, if the results of the matching are not intended to be used and are not used to make decisions concerning the rights, benefits, privileges, or status of specific individuals or to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(ii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, 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 the person or persons;

(iii) matches of tax information pursuant to the Internal Revenue Code of 1986 or for the purpose of intercepting a tax refund due an individual under authority granted by statute;

(iv) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; or

(v) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1)).

(13) RECIPIENT AGENCY. – The term "recipient agency" means any agency, or contractor thereof, receiving records processed as part of an agency activity affecting privacy of a source agency for use in a matching program.

(14) NON-FEDERAL AGENCY. – The term "non-Federal agency" means any State or local government, or agency thereof, that receives records processed as part of an agency activity affecting privacy from a source agency for use in a matching program.

(15) SOURCE AGENCY. – The term "source agency" means any (A) agency that discloses records processed as part of an agency activity affecting privacy to be used in a matching program, or (B) State or local government, or agency thereof, that discloses records to be used in a matching program.

(16) FEDERAL BENEFIT PROGRAM. – The term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash, payments, grants, loans, loan guarantees, or other forms of in-kind assistance to individuals.

(17) FEDERAL PERSONNEL. – The term personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

Sec. 4. General Processing Requirements.

(a) RELEVANT AND NECESSARY. – Each agency shall process only personally identifiable information that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by law or executive order of the President.

(b) DIRECT COLLECTION. – Each agency shall collect personally identifiable information to the extent practicable directly from the data subject when the personally identifiable information may result in adverse determinations about the data subject's rights, benefits, privileges, or status under Federal programs.

(c) NOTICE. – Each agency shall, in writing or otherwise and in understandable language, inform each data subject whom it asks to supply personally identifiable information, at the time of collection and in a manner that allows the data subject to obtain or retain a copy, of the following:

(1) the authority for the collection;

(2) the principal purpose or purposes for which the personally identifiable information will be used;

(3) the agency designated disclosures that may be made of the personally identifiable information; and

(4) whether the data subject is required by law to supply the personally identifiable information and the consequences of not providing all or any part of the personally identifiable information.

(d) DETERMINATIONS. – Each agency shall process records used by the agency in making any determination about a data subject with sufficient accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the data subject in the determination.

(e) DISCLOSURE. – Prior to disclosing any personally identifiable information to any person other than an agency, unless the dissemination is made pursuant to section 552, title 5, United States Code, each agency shall make reasonable efforts to assure that the personally identifiable information is accurate, complete, timely, and relevant for agency purposes.

(f) FIRST AMENDMENT. – No agency shall process a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, or by the individual, or unless pertinent to and within the scope of an authorized law enforcement activity.

(g) LEGAL PROCESS. – Each agency shall make reasonable efforts to serve notice on a data subject when any personally identifiable information about the data subject is made available to any person under compulsory legal process when the process becomes a matter of public record.

(h) SAFEGUARDS. – Each agency shall, consistent with the requirements in subchapter II of chapter 35 of title 44, United States Code, establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any data subject.

Sec. 5. Agency Activity Affecting Privacy.

(a) SCOPE. – Each agency shall determine the scope of each agency activity affecting privacy so as to reflect accurately its processing of records and to do so in a manner that supports public understanding of agency operations.

(b) GUIDANCE. –The Director of the Office of Management and Budget shall issue guidance to agencies about determining the scope of an agency activity affecting privacy. The guidance shall advise agencies how to address these goals to the extent practicable:

(1) the goal of grouping activities with similar or related purposes within the same agency activity affecting privacy;

(2) the goal of grouping activities based on similar authority within the same agency activity affecting privacy;

(3) the goal of keeping records eligible for exemptions separate from non-exempt activities; and

(4) the goal of defining agency activities affecting privacy so that agency designated disclosures do not apply to records unnecessarily.

(c) DESCRIPTION. – For each agency activity affecting privacy, an agency shall prepare and maintain a description that shall include –

(1) the name of the activity, the scope of the activity, each principal substantive purpose that the activity supports, and the authority for the activity, including any related information collection requests approved under the Paperwork Reduction Act;

(2) the name of the agency component primarily responsible for the activity, the principal postal, electronic mail, and website addresses of that component, and the name of other agency components that significantly participate in the activity;

(3) the categories of data subjects about whom records are processed as part of the activity;

(4) the categories of records processed in the activity;

(5) the principal information technologies employed, including any novel or innovative applications of technology; any automated decision making; any processing of records using artificial intelligence; any algorithmic development, analysis, or application; or any similar activities with the potential to affect the rights or interests of data subjects;

(6) each agency designated disclosure applicable to records processed as part of the activity, including a good faith effort to list agency designated disclosures in the approximate order in which they are likely to be used, with the most used disclosure listed first;

(7) the categories of sources of records in the activity, including any commercial, governmental, or other sources that the agency routinely reviews, consults, or otherwise uses to carry out the activity;

(8) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records in the activity, including the name and location of records disposal schedules covering any of the records;

(9) the location of the agency website and of the agency's rules where an individual can learn how to exercise rights available under this Act;

(10) whether the activity is likely to include any records subject to an exemption in section 12 of this Act; describing the reasons exempt records may be included; and describing how the exemption affects any rights available under this Act;

(11) the date the description was most recently published or amended; and

(12) a reference where the agency publishes any personally identifiable information processing diagram for the activity and any publicly available privacy impact assessment conducted by the agency relevant to the activity.

(d) PUBLICATION. – An agency shall publish the following notices, including the description of each agency activity affecting privacy prepared as provided in subsection (c) –

(1) For the initial publication of a description of an agency activity affecting privacy, the agency shall publish a complete notice in the Federal Register as provided in section 553(b) and (c) of title 5, United States Code.

(2) For any material change in an agency activity affecting privacy, including a new or modified purpose or agency designated disclosure, the agency shall –

(A) publish a notice of the proposed change in the activity in the Federal Register as provided in section 553(b) and (c) of title 5, United States Code;

(B) provide, either as part of the Federal Register notice or on the agency's website, the full text of the description of the activity clearly identifying the proposed change; and

(C) if the agency only provides the full text of the description on its website, make the full text available on or before the date when the public comment period begins.

(3) For a non-material change in an agency activity affecting privacy or in an agency designated disclosure, the agency shall publish a notice describing the change in the Federal Register and provide on its website the full text of the revised description of the agency activity affecting privacy that clearly identifies the proposed change.

(e) FULL TEXT REQUIRED. – In any published description or proposed modification of an agency activity affecting privacy or agency designated disclosure, an agency shall include the full text of each agency activity affecting privacy or each agency designated disclosure and not by reference to another document.

(f) JOINT AGENCY ACTIVITIES AFFECTING PRIVACY. – The Director of the Office of Management and Budget shall issue guidance covering any agency activity affecting privacy operated by one agency on behalf of one or more other agencies or for which more than one agency has a responsibility. The guidelines shall prescribe how the requirements of this Act shall be allocated among the agencies involved and how the duties imposed by this Act shall be carried out.

Sec. 6. Allowable Uses and Disclosures.

(a) USE. – An agency may allow those officers and employees of the agency who have a need for a record from an agency activity affecting privacy to use the record in the performance of their duties. Nothing in this subsection expands or reduces the ability of an agency to –

(1) use or withhold from use a record as otherwise provided by statute; or

(2) withhold a record used for one agency function from another agency function.

(b) DISCLOSURE. – No agency shall disclose any record 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 data subject, unless disclosure of the record is otherwise allowed under this section.

(c) AGENCY DESIGNATED DISCLOSURE. – An agency may disclose a record if the disclosure is for an agency designated disclosure adopted by the agency pursuant to section 5.

(d) ALLOWABLE DISCLOSURES. – An agency may disclose a record if the disclosure is the following:

(1) REQUIRED BY FOIA. – The disclosure is required under section 552 of title 5, United States Code.

(2) STATISTICAL AGENCY DISCLOSURE. – The disclosure is to a statistical agency or unit for statistical purposes, as those terms are defined in section 3561 of title 44, United States Code, and subject to the provisions, including the limits on use and disclosure, of section 3572 of title 44, United States Code.

(3) ARCHIVES DISCLOSURE. – The disclosure is to the National Archives and Records Administration –

(A) for a record that has sufficient historical or other value to warrant its continued preservation by the United States Government;

(B) for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has that value; or

(C) pursuant to a records management inspection as provided in chapter 29 of title 44, United States Code.

(4) REQUEST FROM LAW ENFORCEMENT AGENCY. – The disclosure is to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality made a written request to the agency that processes the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

(5) CIVIL OR CRIMINAL LAW ENFORCEMENT. – The disclosure is to the appropriate Federal, State, local, tribal, or foreign agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the record is relevant to a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving agency.

(6) HEALTH OR SAFETY. – The disclosure is to a person if –

(A) the agency believes in good faith that –

(i) the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any individual or the public and

(ii) the person is reasonably able to prevent or lessen the threat; and

(B) the agency making a disclosure under this paragraph sends a notice of the disclosure to the data subject's last known physical or electronic mail address, unless the Chief Privacy Officer determines that sending a notice would be inappropriate and documents the reason for the determination in writing.

(7) CONGRESS. – The disclosure is to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any the joint committee.

(8) WRITTEN INQUIRY TO MEMBER OF CONGRESS. –The disclosure is to a Member of Congress in response to a written inquiry by the Member of Congress after the Member of Congress receives a written request from the data subject pertaining to or concerning a matter contained in the record.

(9) GOVERNMENT ACCOUNTABILITY OFFICE. – The disclosure is to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.

(10) CONTRACTORS, GRANTEES, OTHERS. – The disclosure is to a contractor, grantee, consultant, or volunteer performing or working on a contract, grant, cooperative agreement, or otherwise for the agency and who has a need for the record in the performance of their duties for the agency. When required, the recipient shall comply with section 14.

(11) COURTS AND LITIGATION. – The disclosure –

(A) is pursuant to the order of a court of competent jurisdiction;

(B) occurs in a filing made in a court of competent jurisdiction pursuant to the rules of that court;

(C) is to a party in litigation with the agency, is authorized by the rules or order of the court or adjudicative body conducting the proceeding before which the litigation is pending, and a rule, order, or a signed written agreement, limits use of the disclosed record to the purpose of conducting the litigation; or

(D)(i) is to a party, or potential party, to litigation with the agency, or to the party's authorized representative, or to an independent mediator, in connection with settlement discussions; and

(ii) the disclosure of the record is limited to the purposes of the settlement negotiations by (I) a rule or order of the court or adjudicative body conducting the proceeding, or (II) a written agreement signed by the parties.

(12) DATA BREACH RESPONSE. – The disclosure is –

(A) for the purpose of responding to a suspected or confirmed data breach that involves a risk of harm to an individual or a data system;

(B) approved by –

(i) the head of the agency;

(ii) the Chief Privacy Officer of the agency;

(iii) a senior agency official designated under a written agency data breach response plan; or

(iv) the Federal Chief Privacy Officer;

(C) of records from an agency activity affecting privacy that an agency official supervising the data breach response determines are (i) likely to be relevant to the purpose of this paragraph; and (ii) made to an agency, entity, or other person for which the official approving the disclosure has reason to believe may be able to assist in identifying the existence or scope of a data breach or in responding to the data breach either by providing a remedy for an individual who may have been affected by the data breach or by assisting with protection of a data system; and

(D) pursuant to a contract or agreement limiting the use of all data disclosed to the purpose of the disclosure and requiring either the prompt return or destruction of all data disclosed when the agency determines that the purposes of the disclosure are fulfilled.

(13) FEDERAL PERSONNEL AND OTHER DECISIONS. – The disclosure is to those officials and employees of a Federal agency or Federal entity that require personally identifiable information relevant to a decision about (i) the hiring, appointment, or retention of an employee; (ii) the issuance, renewal, suspension, or revocation of a security clearance; (iii) a security or suitability investigation; (iv) the awarding of a contract or grant; or (v) the issuance of a grant or benefit.

(e) MINIMIZE ALLOWABLE DISCLOSURES. – When disclosing a record pursuant to an allowable disclosure in subsection (d), an agency shall make a good faith effort to disclose the minimum amount of personally identifiable information that will accomplish the purpose of the disclosure.

(f) PROCEDURAL REQUIREMENTS FOR AGENCY DESIGNATED DISCLOSURES.

(1) CPO APPROVAL. All agency designated disclosures must be approved by the agency's Chief Privacy Officer pursuant to section 9(b)(6);

(2) DESCRIPTION. – When establishing an agency designated disclosure, the agency shall to the extent practicable identify as part of the description of the disclosure –

(A) why the disclosure qualifies under one or more of the subparagraphs (A), (B), and (C) in the definition of "agency designated disclosure" in section 3(9);

(B) the class of recipients of personally identifiable information;

(C) the types of personally identifiable information that may be disclosed;

(D) the purpose of and authority for the disclosure, including a good faith effort to specify each statute or treaty that requires or specifically authorizes disclosure of personally identifiable information;

(E) the position description or function of those agency officers and employees who may authorize a disclosure as an agency designated disclosure.

(3) MINIMIZING DISCLOSURE. –

(A) When establishing an agency designated disclosure, an agency shall as part of the description of the disclosure and to the extent practicable, limit each agency designated disclosure to those records and to those portions of records processed in an agency activity affecting privacy that fulfill the purpose for which the agency designated disclosure was established;

(B) When disclosing a record pursuant to an agency designated disclosure, an agency shall to the extent practicable disclose the minimum amount of personally identifiable information that will accomplish the purpose of the disclosure.

(4) PUBLIC DISCLOSURE. – If an agency designated disclosure authorizes the public disclosure of personally identifiable information, the agency shall establish a procedure that requires the approval of the Chief Privacy Officer prior to the disclosure. This paragraph does not apply to disclosures required by section 552 of title 5, United States Code, or to other public disclosures required by law.

(g) OMB GUIDANCE. –

(1) ALTERNATIVE TO CONSENT. – The Director of the Office of Management and Budget shall issue guidance discouraging agencies from establishing agency designated disclosures principally as an alternative to obtaining consent of the data subject.

(2) MODEL NOTICES. – The Director of the Office of Management and Budget may prepare and publish for the use of agencies model notices of agency designated disclosures that are likely to be relevant to many agencies. Any agency that proposes to adopt an agency designated disclosure addressing disclosures covered by a model notice published in accordance with this paragraph that differs from the model notice by allowing for broader or additional disclosures shall explain its reasons when it publishes the agency designated disclosure for public comment.

(h) LIMITS. – Except as otherwise provided by law, nothing in this Act requires an agency to disclose a record to anyone other than the data subject or to a parent, guardian, or other person identified in section 16(d).

Sec. 7. Access to and Amendment of Records.

(a) ACCESS. – (1) An agency shall upon request by a data subject regarding a record processed as part of an agency activity affecting privacy permit the data subject and any person chosen by the data subject to review the record and to have a copy of any or all of the record in any form or format requested by the data subject if the record is readily reproducible by the agency in that form or format.

(2) An agency shall acknowledge in writing or by electronic mail receipt of a request under this subsection within ten days of receipt and shall provide the requested record within 30 days. If the request is denied in whole or in part, the agency shall inform the data subject of the denial, the reason for the denial, and the procedures established by the agency for appealing the denial to the head of the agency or designee.

(3) If after an appeal of a denial of a request for review or copy of a record, the agency refuses to provide the review or copy, the agency shall inform the data subject of the reasons for the denial and of the procedures for judicial review.

(4) For any request under this subsection and section 8(b)(2), an agency shall also provide to a data subject any requested information that would be available to the data subject under section 552 of title 5, United States Code.

(b) AMENDMENT. – (1) An agency shall upon request by a data subject permit the data subject to request amendment of a record processed as part of an agency activity affecting privacy pertaining to the data subject that the data subject believes is not accurate, relevant, timely, or complete.

(2) An agency shall acknowledge in writing or by electronic mail receipt of a request under this subsection within ten days of receipt and shall within 30 days of the receipt of the request, either –

(A) make any amendment that the data subject requested, and promptly inform the data subject of the amendment; or

(B) inform the data subject of its refusal to make the requested amendment, the reason for the refusal, the procedures established by the agency for appealing the refusal to the head of the agency or designee.

(3) An agency shall within 30 days of the receipt of an appeal by the data subject of a denial of a request for amendment either –

(A) make any amendment that the data subject requested, and promptly inform the data subject of the amendment; or

(B) inform the data subject of –

(i) the right to file with the agency a concise statement setting forth the reasons for the data subject's disagreement with the refusal of the agency; and

(ii) the right to judicial review of the denial.

(4) In any future disclosure of a record or portion of a record about which a data subject filed a statement of disagreement, the agency shall clearly identify any disputed information and, unless the data subject objects in writing, provide a copy of the data subject's statement of disagreement and, if the agency chooses, a statement describing the agency's reasons for not making the amendment requested.

(c) EXTENSION. – The Chief Privacy Officer may extend the deadlines for responding to a request under this section for (1) review or a copy of a record, or (2) for an amendment, in each case by no more than 30 days, by notifying the data subject making a request in writing or by electronic mail.

Sec. 8. Disclosure History

(a) ACCURATE DISCLOSURE HISTORY REQUIRED. – Each agency, with respect to each agency activity affecting privacy, shall except for uses made under section 6(a) and disclosures made under section 6(d)(1), keep or maintain the ability to create upon request an accurate history of –

(1) the date, nature, and purpose of each disclosure of a record to any person or to another agency made pursuant to an agency designated disclosure; and

(2) the name and address of the person or agency to whom the disclosure is made;

(b) RETENTION, AVAILABILITY, AND NOTICE OF DISCLOSURE HISTORY. – Each agency shall –

(1) keep or maintain the ability to create upon request a disclosure history for at least five years after the disclosure or for the life of the record, whichever is longer;

(2) except for disclosures made under section 6(d)(2), (3), (4) and (5), make the disclosure history available to the data subject upon a request made pursuant to the access procedure described in section 7(a); and

(3) inform any person or other agency about any amendment or statement of disagreement made in accordance with section 7 of any record previously disclosed to the person or agency if a disclosure history is available, if the data subject who requested the amendment or submitted a statement of disagreement asks that the amendment or statement be disclosed.

Sec. 9. Chief Privacy Officer.

(a) CHIEF PRIVACY OFFICER. – The head of each agency shall, promptly after the effective date of this Act, designate a Chief Privacy Officer to carry out the functions assigned under this Act and other related functions. If another statute established a privacy officer or similar officer for the agency, the head of the agency may designate that officer to carry out the functions assigned under this Act.

(b) DUTIES. – The Chief Privacy Officer for an agency shall –

(1) have agency-wide responsibility for privacy and for compliance with fair information practices;

(2) have agency-wide responsibility for overseeing agency compliance with Federal laws, regulations, and policies relating to privacy, including primary responsibility for implementation of this Act;

(3) participate in identifying and addressing privacy risks throughout the agency;

(4) have responsibility for agency privacy impact assessments as provided in section 11;

(5) have a central role in the agency's development and evaluation of legislative, regulatory, and other policy proposals relating to or affecting the privacy of personally identifiable information; and

(6) approve the publication of the description of each agency activity affecting privacy, including each agency designated disclosure, prior to publication for comment and before the description and the agency designated disclosure becomes final.

(c) NOTICES. –The Chief Privacy Officer shall, to the extent practicable, standardize elements and terminology of notices of agency activities affecting privacy, including agency designated disclosures.

(d) Personally Identifiable Information Processing Diagram. – The Chief Privacy Officer shall, to the extent practicable, maintain on the agency privacy website for each major agency activity affecting privacy a current personally identifiable information processing diagram or equivalent document that visually depicts the collection, use, and disclosure of personal information and that shows the principal sources of information, the principal internal users of the personal information, the principal purposes for which the agency collects and discloses personal information, and the recipients of the disclosures.

(e) REPORT. –When the Chief Privacy Officer of an agency determines that a threat or vulnerability is creating or is likely to create a significant disruption to the privacy responsibilities of the agency, a serious unresolved privacy or security risk to the agency, or an inappropriate or avoidable serious privacy or security risk to data subjects, the Chief Privacy Officer may –

(1) consult with the Chief Information Officer of the agency; and

(2) report from time to time directly to the head of the agency.

(f) GUIDANCE. –The Director of the Office of Management and Budget may issue guidance on the activities and functions of a Chief Privacy Officer, including guidance on the preparation and format of personally identifiable information processing diagrams prepared under subsection (d).

Sec. 10. Federal Chief Privacy Officer at the Office of Management and Budget.

(a) FEDERAL CHIEF PRIVACY OFFICER. –The Director of the Office of Management and Budget shall, promptly after the effective date of this Act, establish an Office of the Federal Chief Privacy Officer as part of the Office of Information and Regulatory Affairs. A Federal Chief Privacy Officer shall head the Office of the Federal Chief Privacy Officer.

(b) DUTIES. –The Office of the Federal Chief Privacy Officer shall –

(1) have responsibility for preparing Office of Management Budget guidance under this Act;

(2) provide notice and opportunity for public comment for the guidance;

(3) assist and direct agencies with the transition from compliance with the Privacy Act of 1974 to compliance with this Act;

(4) oversee agency compliance with this Act and provide continuing assistance to agencies with the implementation of this Act; and

(5) have responsibility for advising the Director on all privacy matters.

Sec. 11. Privacy Impact Assessment Process.

(a) PURPOSE. – The purposes of the privacy impact assessment process are –

(1) to inform agency decisions for the life cycle of agency activities affecting privacy, including planning, design, implementation, and conduct, in a manner consistent with other Federal information resources management policies, principles, standards, and guidelines;

(2) to identify significant risks to the agency and significant consequences for the privacy of data subjects from the conduct of agency activities affecting privacy;

(3) to seek and implement ways to minimize significant risks and consequences prior to establishing or modifying an agency activity affecting privacy while providing for the efficient and effective conduct of agency responsibilities;

(4) to provide that agency processing of personal information minimizes the processing of personally identifiable information, maximizes fairness, includes appropriate due process protections, and generally complies with fair information practices;

(5) to provide to the extent practicable an opportunity for public comment in the planning and design of an agency activity affecting privacy;

(6) to complete the process, to the extent practicable, before the agency makes final decisions about the design of an agency activity affecting privacy; and

(7) to document the conduct of the process with a written report.

(b) PROCESS. –

(1) Each agency shall conduct either a thorough or a limited privacy impact assessment process for new or significantly modified agency activities affecting privacy and for new or significantly revised matching programs.

(2) In determining whether to conduct a thorough or a limited privacy impact assessment process, an agency shall consider using a thorough assessment when agency activities affecting privacy are reasonably likely to have one or more of these characteristics:

(A) affect a large number of data subjects;

(B) involve determinations of eligibility for rights, benefits, privileges, or status;

(C) employ or propose to employ any novel or innovative applications of technology;

(D) present significant risks to the agency or significant consequences for the privacy of data subjects;

(E) involve the routine collection of records from sources outside the Federal government or the routine disclosure of records outside the Federal government; or

(F) result in significant new mergers of previously separate government databases.

(3) The Director of the Office of Management and Budget shall issue guidance to help agencies –

(A) decide whether to conduct either a thorough or a limited privacy impact assessment process;

(B) establish priorities for conducting privacy impact assessment processes;

(C) address privacy –

(i) as part of the information and information system life cycles;

(ii) in relation to other requirements pertaining to the collection of information; and

(iii) with regard to information system development, security, and the use of information technology resources;

(D) determine when and how to conduct public consultations;

(E) conduct a privacy impact assessment process for an agency activity affecting privacy that involves more than one agency; and

(F) conduct any other aspect of the privacy impact assessment process.

(c) MANAGING THE PRIVACY IMPACT ASSESSMENT PROCESS.

(1) The Chief Privacy Officer shall determine the scope of each privacy impact assessment process, including deciding whether a thorough or limited process is appropriate; which agency activities affecting privacy should be included in which privacy impact assessment process; identify the agency components that shall participate in the process; establish a timetable for the process; and manage any public notice and public participation.

(2) Each privacy impact assessment process shall result in a final written report.

(3) If an agency activity affecting privacy involves classified information or other information unsuitable for public disclosure under existing laws and Executive Orders, the agency shall disclose publicly as much about the privacy impact assessment process as practicable.

(4) If in the judgment of the Chief Privacy Officer, it is not practical to complete a privacy impact assessment process before an agency begins or significantly changes an activity that would otherwise require a privacy impact assessment process, the Chief Privacy Officer may delay or

otherwise adjust the conduct of the process and the timing and form of public report in a suitable manner. The Chief Privacy Officer shall provide public notice of any delay or adjustment on the agency privacy website.

(5) The Chief Privacy Officer shall send to appropriate Committees of Congress a copy of each interim and final written report on each major privacy impact assessment.

(d) ELEMENTS OF A PRIVACY IMPACT ASSESSMENT PROCESS.

(1) An agency conducting a thorough privacy impact assessment process shall, to the extent practicable, include –

(A) an identification of risks to the agency from the processing of records, including a description of ways to manage and to mitigate the risks and a justification for the final choices made by the agency;

(B) an identification of information technology available to support the processing of records, including a justification for the final choices made by the agency;

(C) an analysis of the risks and consequences of the activity for privacy of data subjects, including expected uses and disclosures; a description of possible ways to mitigate the consequences and risks; and a justification for the final choices made by the agency; and

(D) a description of efforts to seek public and stakeholder participation in the privacy impact assessment process and a response by the agency to public and stakeholder comments.

(2) An agency conducting a limited privacy impact assessment process shall, to the extent practicable, include –

(A) an explanation of the reasons that the agency decided to conduct a limited rather than a thorough privacy impact assessment process;

(B) a description of the risks and consequences of processing of records for the agency and for data subjects;

(C) a description of alternatives considered;

(D) a justification for the final choices made by the agency; and

(E) a summary of any public and stakeholder participation and comments.

(e) PUBLIC NOTICE AND PARTICIPATION. The Chief Privacy Officer of an agency shall, to the extent practicable, provide for public notice of each privacy impact assessment process and for public comment or other public participation in the process. The Chief Privacy Officer may provide public notice through the privacy website of the agency or through the Federal Register.

(f) PUBLIC LAW 107-437. – An agency or component that completed the transition to this Act shall not comply with section 208(b) of Public Law 107-437, 44 United States Code § 3501 note.

Sec. 12. Exemptions

(a) LIMITS ON ACCESS. – Nothing in this Act shall allow an individual a right of access to a record or a disclosure history record, or a right of amendment of (1) any information compiled in reasonable anticipation of a civil action or proceeding, (2) any classified information; (3) data or information acquired by an agency under a pledge of confidentiality and used or disclosed for exclusively statistical purposes pursuant to section 3572 of title 44, United States Code; (4) any information created as testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if disclosure would compromise the objectivity or fairness of the testing or examination process; or (5) information that was exempt from disclosure under section 552a of title 5, United States Code, as information collected prior to the

effective date of section 3 of the Privacy Act of 1974 (Public Law No. 93-579) under an implied promise that the identity of the source would be held in confidence.

(b) PERSONNEL INVESTIGATIONS AND EVALUATIONS. – An agency is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record with respect to any information that would identify a confidential source who furnished information to the Government under an express promise that the identity of the source would be held in confidence if the information was created as –

(1) investigatory material solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information.

(2) evaluation material to determine potential for promotion in the armed services.

(c) INVESTIGATORY MATERIAL FOR LAW ENFORCEMENT PURPOSES. –

(1) An agency is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record, for investigatory information compiled for law enforcement purposes unless the individual is denied any rights, benefits, privileges, or status that the individual would otherwise be entitled to by Federal law, or for which the individual would otherwise be eligible, as a result of the maintenance of the information.

(2) Any right of access, right of amendment, or a disclosure history record in section 7 and section 8 that an individual would have as a result of a denial of any rights, benefits, privileges, or status as described in paragraph (1) of this subsection shall not apply to –

(A) the extent that the disclosure of the material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence;

(B) information exempt from disclosure pursuant to subsection (a)(5) of this section; or

(C) information that qualifies for exemption as criminal law enforcement information in subsection (f).

(d) PROTECTIVE SERVICES. –An agency activity affecting privacy operated by an agency in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18, United States Code, is exempt from the requirement in subsection (a) of section 4 to process only relevant and necessary information, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record to the extent that records in the agency activity affecting privacy relate to those protective services.

(e) INTELLIGENCE AGENCIES. –

(1) An intelligence agency or component thereof defined as part of the Intelligence Community pursuant to section 3003, title 50, United States Code is exempt from –

(A) the requirements to comply with subsections (a), (b), (c), and (d) of section 4; and

(B) the requirements in section 7 and section 8 to provide an individual a right of access, right of amendment, or a disclosure history record.

(f) CRIMINAL LAW ENFORCEMENT AGENCIES. – A criminal law enforcement agency or component thereof that performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend

criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, is exempt from the requirement to comply with subsections (a), (b), (c), and (d) of section 4, and from the requirements in section 7 and section 8 to provide an individual a right of access, a right of amendment, or a disclosure history record with respect to any records that consist of –

(1) 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;

(2) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or

(3) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

(g) NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. – Any record subject to this Act accepted by the National Archives of the United States as a record with sufficient historical or other value to warrant its continued preservation by the United States Government pursuant to section 2107 of title 44, United States Code, and that the Archivist of the United States processes pursuant to section 2108 of title 44 United States Code, shall not be subject to any of the requirements of this Act.

(h) GENERAL REQUIREMENTS. –

(1) When publishing a notice of an agency activity affecting privacy that includes a record exempt or potentially exempt under provisions of this section, an agency shall, to the extent practicable, describe the activities that qualify for the exemption and distinguish exempt and non-exempt records and activities. The agency shall include in the notice the reasons the agency expects to utilize the exemptions.

(2) In applying an exemption available under this section, an agency shall restrict application of the exemption to those records and activities that include information that the exemption seeks to protect.

(3) If an agency discloses a record exempt under this section from any provision to another agency, the record shall continue to be exempt in the same manner and to the same extent as if the disclosing agency continued to process the record. An agency transferring an exempt record shall identify for the recipient agency the part of the record that qualifies for exemption and the nature and scope of the exemption.

(i) WAIVERS. – An agency processing a record that qualifies for exemption in this section may take one or more of the following actions –

(1) waive application of an exemption, in whole or in part, by including the waiver in the description required in section 5(c) of an agency activity affecting privacy;

(2) issue a regulation defining when the agency may waive application of an exemption, in whole or in part; and

(3) waive application of an exemption in whole or in part or on a case-by-case basis.

Sec. 13. Criminal and Other Penalties

(a) OFFENSES. –

(1) Any person who knowingly and willfully and in violation of this Act and under false pretenses obtains a record that contains personally identifiable information shall be punished as provided in subsection (b).

(2) Any officer, employee, contractor, grantee, or volunteer of an agency, or other person who by virtue of employment, official position, or contract has possession of, or access to, a record that contains personally identifiable information the disclosure of which is prohibited by this Act or by rules or regulations established thereunder, and who knowing that disclosure of the record is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be punished as provided in subsection (b).

(b) PENALTIES. – A person described in subsection (a) shall –

(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed with intent to sell, transfer, or use a record that contains personally identifiable information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

(c) PUBLISHING. – Any officer or employee of any agency who willfully establishes or maintains an agency activity affecting privacy without meeting the requirements in section 3 to publish a description of the agency activity affecting privacy shall be guilty of a misdemeanor and fined not more than $5,000.

(d) ADVERSE PERSONNEL ACTIONS. – An officer or employee of an agency who processes records in violation of this Act shall be subject to appropriate administrative discipline including, when circumstances warrant, suspension from duty without pay or removal from office.

Sec. 14. Government Contracts, Grants, and Cooperative Agreements.

When an agency provides by a contract, grant, cooperative agreement, or otherwise for the conduct of an agency activity affecting privacy to accomplish an agency function, whether in whole or in part, the agency shall, consistent with its authority, cause the requirements of this Act to be applied to the activity. The agency shall be responsible for any publication, notice, or rule required under this Act with respect to that agency activity affecting privacy.

Sec. 15. Matching.

(a) MATCHING AGREEMENTS. –

(1) CONTENTS OF MATCHING AGREEMENTS. – A source agency shall not disclose a record processed as part of an agency activity affecting privacy for use in a matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency receiving the records, specifying –

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings from the operation of the program;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter. to data subjects whose records are used in the activity that any information provided by the data subjects may be subject to verification through matching programs;

(E) procedures for verifying information produced in the matching program as required by this section;

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in the matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of the programs;

(H) prohibitions on duplication and redisclosure of records imposed by the source agency on the recipient agency or the non-Federal agency, except where duplication or redisclosure is required by law or essential to the conduct of the matching program;

(I) procedures governing the use by the recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return or destruction of the records used in the program;

(J) information on assessments that have been made on the accuracy of the records that will be used in the matching program;

(K) that the Comptroller General may have access to all records of a recipient agency or non-Federal agency receiving the records as the Comptroller General deems necessary in order to monitor or verify compliance with the agreement;

(L) a provision requiring revision or termination of the agreement if the need for, circumstances relating to, or the law regarding any aspect of the matching agreement changes in a material way during course of the agreement; and

(M) the expiration date for the agreement, which can be no later than five years after the agreement took effect.

(2) CERTIFICATION OF MATCHING AGREEMENT. – No matching agreement shall take effect unless the Chief Privacy Officer of the source agency certifies in writing that –

(A) the agreement complies with all requirements of this Act;

(B) the Chief Privacy Officer of the source agency consulted with the agency Inspector General, Chief Information Officer, Chief Data Officer, and senior officials from the office providing or using records for the matching program activity about the justification for the matching program;

(C) any findings of the agency Inspector General or the Government Accountability Office relevant to the matching program were adequately taken into account in the agreement;

(D) any problems identified in previous matching programs between the same agencies were adequately addressed;

(E) except for matching programs mandated by statute, in the judgment of the Chief Privacy Officer of the source agency, the sharing of records pursuant to the matching agreement is financially justified based on any relevant results of current or past matching programs; and

(F) except for matching programs mandated by statute, in the judgment of the Chief Privacy Officer of the source agency, the matching program is in the public interest.

(3) PRIOR COMPLIANCE REQUIRED. – No source agency may enter into a second or subsequent matching agreement unless –

(A) the recipient agency or non-Federal agency receiving the records certifies in writing that it complied with the provisions of previous agreements; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(4) POSTING. – A copy of each matching agreement and a copy of the certification of the Chief Privacy Officer shall be posted on the website of the source agency and sent to the Director of the Office of Management and Budget.

(5) EFFECTIVE DATE OF AGREEMENT. – No matching agreement shall be effective until 30 days after the date on which a copy is posted on the agency website.

(6) SECTION NOT AUTHORITY TO CONDUCT PROGRAMS. – Nothing in this section may be construed to authorize –

(A) any matching programs not otherwise authorized by law; or

(B) disclosure of records for a matching program except to a Federal, State, or local agency.

(b) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS. –

(1) TIME FOR NOTICE AND RESPONSE. – In order to protect an individual whose record is used in a matching program, no source agency or non-Federal agency using a record from a matching program may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to the individual, or take other adverse action against the individual, as a result of information produced by the matching program, until –

(A)(i) the source agency has independently verified the information; or

(ii) the Chief Privacy Officer of the source agency determines in accordance with guidance issued by the Director of the Office of Management and Budget that–

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) the Chief Privacy Officer of the source agency has a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest the findings; and

(C) the expiration of –

(i) any time period established by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no the period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) BASIS FOR ADVERSE ACTION. – The independent verification referred to in paragraph (1)(A)(i) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of–

(A) the amount of any asset or income involved;

(B) whether the individual actually has or had access to the asset or income for the individual's own use; and

(C) the period or periods when the individual actually had the asset or income.

(3) HEALTH AND SAFETY EXCEPTION. – Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by the paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by the paragraph.

Sec. 16. Miscellaneous.

(a) WAIVER. – A waiver of the rights provided under section 7 and section 8 of this Act is against public policy and is void and unenforceable.

(b) SALE OF PERSONALLY IDENTIFIABLE INFORMAITON. – An individual's name; postal and electronic addresses; telephone numbers; and other personally identifiable information may not be sold or rented by an agency unless specifically authorized by statute. This provision shall not be construed to require the withholding of personally identifiable information otherwise permitted to be made public.

(c) EFFECT OF OTHER LAWS. –

(1) FOIA EXEMPTIONS NOT APPLICABLE TO RIGHTS UNDER THIS ACT. – No agency shall rely on any exemption contained in section 552 of title 5, United States Code, to withhold from an individual any record that is otherwise accessible to the individual under the provisions of this Act.

(2) EXEMPTIONS UNDER THIS ACT NOT APPLICABLE TO FOIA. – No agency shall rely on any exemption in this Act to withhold from an individual any record that is otherwise accessible to the individual under the provisions of section 552 of title 5, United States Code.

(d) RIGHTS OF PARENTS AND GUARDIANS. – A parent, guardian, other person acting in loco parentis, or person with a valid power of attorney who under applicable law has authority to act on behalf of an individual may act on behalf of the individual under this Act.

(e) REPORT TO CONGRESS. – Each agency that proposes to establish or make a change in an agency activity affecting privacy that significantly limits or otherwise alters the rights and opportunities available to individuals under this Act, or that adds or significantly modifies an agency designated disclosure shall provide adequate advance notice to appropriate Committees of Congress and to the Office of Management and Budget.

(f) WEBSITE. – Each agency shall maintain a privacy website, with appropriate search, indexing, and finding aids, that allows for the full search and downloading of text maintained on the website. The website shall include –

(1) the notice for each current agency activity affecting privacy and any personally identifiable information processing diagram prepared in accordance with section 9(d) of this Act.

(2) a complete history of all changes made in the past ten years to the notice of each agency activity affecting privacy, including the full text of each prior published notice, an identification of all changes, and date on which each change took effect;

(3) a complete list of all Federal Register notices, including all amendments, for each agency activity affecting privacy, together with an electronic or digital link to each notice;

(4) the text of all system of records notices and amendments published under the Privacy Act of 1974 for the ten-year period before completion of the agency transition to compliance with this Act;

(5) information about, and to the extent practicable, a copy of each privacy impact assessment report completed in the past twenty-years or currently being conducted;

(6) other information determined by the head of the agency or by the Chief Privacy Officer to be helpful to the public in understanding agency privacy activities, the provisions of this Act, and the exercise of privacy rights granted by this Act to individuals; and

(7) information about the agency's plans for transition from compliance with the Privacy Act of 1974 to compliance with this Act.

(g) STATUTE OR TREATY. – The failure of an agency to identify a statute or treaty requiring or specifically authorizing disclosure of a record in any notice or publication under this Act shall not overcome any requirement or authorization to disclose the record as provided in the statute or treaty.

Sec. 17. Agency Rules

(a) AGENCY RULES. – In order to carry out the provisions of this Act, each agency that maintains an agency activity affecting privacy shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of title 5, United States Code, that shall –

(1) establish procedures whereby an individual can be notified in response to the individual's request if any agency activity affecting privacy identified by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for authenticating the identity of a data subject who requests a record or information pertaining to the data subject before the agency shall make the record or information available to the data subject;

(3) establish procedures for the disclosure to a data subject upon request the data subject's record~~;~~

(4) establish procedures for reviewing a request from a data subject for amendment of any record or information, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for a data subject to be able to exercise fully the data subject's rights under this Act;

(5) describe any limits that apply to the exercise of rights under this Act as a result of exemptions and including the name of any agency activity affecting privacy to which exemptions apply;

(6) establish fees to be charged, if any, to a data subject for making a copy of records requested under this Act, excluding the first 1000 pages of records provided on paper, any record provided in electronic form or format, and the cost of search for and review of the records; and

(7) establish rules of conduct for persons involved in the design, development, conduct, or maintenance of any agency activity affecting privacy, or in processing any personally identifiable information, and instruct each person about the rules and the requirements of this Act and the penalties for noncompliance.

(b) COMPILATION. – The Office of the Federal Register shall biennially compile and publish on a public website available without charge the rules promulgated under this Act and agency descriptions of agency activities affecting privacy published under section 4 of this Act, together with appropriate search, indexing, and finding aids.

Sec. 18. Civil Remedies.

(a) REMEDY. – A data subject may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this section, whenever any agency –

(1) fails to comply with the data subject's request under section 7(a) or section 8(b)(2) of this Act;

(2) decides after review not to amend the data subject's record in accordance with the data subject's request under section 7(b) of this Act, or fails to make the review in conformity with that section;

(3) fails to process any record concerning the data subject with sufficient accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, benefits, privileges, or status, of the data subject that may be made on the basis of the record, and consequently a determination is made which is adverse to the data subject; or

(4) fails to comply with any other provision of this Act, or any rule promulgated thereunder, in a way that has an adverse effect, including mental or emotional distress, on the data subject.

(b) APPEAL.

(1) INJUNCTION TO PROVIDE RECORDS. –In any suit brought with respect to a failure described in subsection (a)(1), the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld. The court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in section 12 of this Act. The burden is on the agency to sustain its action.

(2) INJUNCTION TO AMEND RECORDS. – In any suit brought with respect to a decision or failure described in subsection (a)(2), the court may order the agency to amend the data subject's record in accordance with the data subject's request or in any other way as the court may direct. The court shall determine the matter de novo.

(3) DAMAGES AND COSTS. – In any suit brought with respect to a decision or failure described in subsection (a)(3) or (a)(4) in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the data subject for –

(A) provable damages, including mental or emotional distress, sustained by the data subject as a result of the refusal or failure or $1000, whichever is greater, but in any class action, the court may reduce the damage award if the total damages are excessive or otherwise unwarranted; and

(B) the costs of the action together with reasonable attorney fees and other litigation costs as determined by the court;

(4) VENUE AND STATUTE OF LIMITATIONS. – An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or in which the complainant has a principal place of business, or in which the agency headquarters are located, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that if an agency materially and willfully misrepresented any information required under this Act to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this Act, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

Sec. 19. Administrative Remedy.

(a) COMPLAINT. –

(1) Any person may file with the Chief Privacy Officer of the agency a complaint setting forth specific facts alleging that an agency failed to comply in a material way with this Act, including any provision regulating –

(A) publication of a timely and accurate description of an agency activity affecting privacy;

(B) a properly defined and adopted agency defined disclosure;

(C) a meaningful and timely privacy impact assessment process;

(D) matching programs; or

(E) any other action specified in this Act.

(3) The Chief Privacy Officer of the agency shall –

(A) acknowledge receipt of a complaint under this subsection in writing within ten days;

(B) within 90 days, either (i) reject a complaint that lacks sufficient specificity to adequately identify or support the allegations in the complaint or that lacks merit, and promptly notify the complainant of the right to appeal under this section, or (ii) if any allegations in the complaint are found to be meritorious, promptly inform the complainant of that decision and undertake reasonable steps to correct any identified deficiencies.

(b) JUDICIAL REVIEW. –

(1) ACTIONS AUTHORIZED. – A complainant whose complaint under this section –

(A) was denied in whole or in part by the agency;

(B) was determined to be meritorious, but on which the agency unreasonably delayed corrective actions; or

(C) did not receive a substantive response from the agency within three months after filing the complaint –

may bring a civil action against the agency to obtain judicial review pursuant to sections 701 through 705 of title 5, United States Code, and the district courts of the United States shall have jurisdiction in the matter.

(2) VENUE. – An action under this section may be brought in the district court of the United States in the district in which the complainant resides, or has a principal place of business, or in which the agency headquarters are located, or in the District of Columbia, without regard to the amount in controversy.

(3) ORDERS. – The court may order the agency to correct any material failure to comply with this Act.

(4) COSTS. –The court may assess against the United States the costs of the action together with reasonable attorney fees and other litigation costs as determined by the court in any case under this section in which the complainant has substantially prevailed.

Sec. 20. Effective Date and Transition.

(a) EFFECTIVE DATE. – This Act shall take effect ten days after the date of enactment. Agencies shall comply with this Act as provided in this section.

(b) TRANSITION. – Within one year after the effective date of this Act, each agency subject to the Privacy Act of 1974 shall prepare a transition plan for changing its privacy compliance activities from section 552a of title 5, United States Code, to this Act. Each agency shall send a copy of its plan to the Director of the Office of Management and Budget and shall post a copy of its plan on the agency's privacy website.

(c) TRANSITION PLAN. – The transition plan –

(1) shall establish a date when all components of the agency will comply with this Act, not to exceed five years from the date of enactment;

(2) shall provide for the promulgation of agency rules required by this Act before any part of the agency completes the transition;

(3) shall provide for publication of a notice disclosing the date of transition in the Federal Register at least 30 days before the date when all or part of the agency completes the transition to this Act;

(4) shall, not less frequently than every six months until the transition for the entire agency is complete, provide for public notice of the progress of the agency's transition on the agency's privacy website;

(5) may provide different transition dates for different agency components.

(d) PRIVACY IMPACT ASSESSMENT DURING TRANSITION. – (1) An agency may choose not conduct a privacy impact assessment process as provided in section 11 before it first establishes an agency activity affecting privacy during the transition to compliance with this Act if the agency determines that –

(A) a recent privacy impact assessment substantially accomplished the purposes set out in section (11)(a) for the agency activity affecting privacy; or

(B) the agency activity affecting privacy only requires a limited privacy impact assessment and the activity is comparable to an activity covered by a privacy impact assessment conducted during the five years before the initial establishment of the activity.

(2) In determining priorities and allocating resources for privacy impact assessment processes during the transition, the agency shall give priority to new agency activities affecting privacy, to activities that are likely involve greater risk to the agency or to data subjects, and to any novel or innovative applications of technology.

(e) TERMINATION. – An agency or agency component that completes the transition from the section 552a of title 5, United States Code, to this Act shall terminate compliance with section 552a of title 5, United States Code, on the transition date for the agency or agency component.

(f) OFFICE OF MANAGEMENT AND BUDGET. –

(1) The Director of the Office of Management and Budget shall issue guidance to agencies regarding the transition from section 552a of title 5, United States Code, to this Act.

(2) Upon the request of an agency, the Director of the Office of Management and Budget may allow the agency to amend its transition plan and to take additional time to complete the transition. No extension may be granted beyond seven years from the date of enactment of this Act.

(3) Until the transition is complete for all agencies, the Director of the Office of Management and Budget shall report annually to the Congress and to the public on the government's progress in transitioning to compliance with this Act.

(g) LITIGATION. – Any litigation initiated under the section 552a of title 5, United States Code, shall be unaffected by this Act and shall continue under the provisions of the section 552a of title 5, United States Code, notwithstanding whether the agency completed its transition to this Act.

Appendix 2. The Privacy Act of 1974

Title 5, United States Code

§552a. Records maintained on individuals

(a) Definitions.- For purposes of this section -

(1) the term "agency" means agency as defined in section 552(e) 1 of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(8) the term "matching program"-

(A) means any computerized comparison of-

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of-

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(B) but does not include-

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, 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;

(iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches-

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1));

(ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or

(x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014;

(9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term "non-Federal agency" means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) Conditions of Disclosure. - No 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, unless disclosure of the record would be -

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

(c) Accounting of Certain Disclosures. - Each agency, with respect to each system of records under its control, shall -

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of -

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to Records. - Each agency that maintains a system of records shall -

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and -

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either-

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the

reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) Agency Requirements. - Each agency that maintains a system of records shall -

(1) 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;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include-

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) 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;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) Agency Rules. - In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall -

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) Civil Remedies. - Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of-

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of Legal Guardians. - For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) Criminal Penalties .- Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established

thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

(j) General Exemptions. - The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is -

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, 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.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific Exemptions. - The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is -

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(l)(1) Archival Records. - Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m)(1) Government Contractors. - When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of title 31 shall not be considered a contractor for the purposes of this section.

(n) Mailing Lists. - An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) Matching Agreements. - (1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying -

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to-

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel,

that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

(E) procedures for verifying information produced in such matching program as required by subsection (p);

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

(J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and

(K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2)(A) A copy of each agreement entered into pursuant to paragraph (1) shall-

(i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and

(ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if-

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) Verification and Opportunity to Contest Findings. - (1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until -

(A)(i) the agency has independently verified the information; or

(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that-

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of-

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) Sanctions. - (1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless-

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) Report on New Systems and Matching Programs.-Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of

Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) Biennial Report. - The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report -

(1) describing the actions of the Director of the Office of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;

(2) describing the exercise of individual rights of access and amendment under this section during such years;

(3) identifying changes in or additions to systems of records;

(4) containing such other information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t)(1) Effect of Other Laws. - No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) Data Integrity Boards. - (1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board-

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including-

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.2

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5)(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget

to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that-

(i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;

(ii) there is adequate evidence that the matching agreement will be cost-effective; and

(iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) In the reports required by paragraph (3)(D), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) Office of Management and Budget Responsibilities. - The Director of the Office of Management and Budget shall -

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

(w) Applicability to Bureau of Consumer Financial Protection. - Except as provided in the Consumer Financial Protection Act of 2010, this section shall apply with respect to the Bureau of Consumer Financial Protection.

*****

Appendix 3. Codification Notes for 5 U.S.C. § 552a

Introduction: The codification notes for a statute contain a wealth of information about the history of a law, the amendments to the law, cross references, effective dates, short titles, and administrative actions implementing a law. In their online form at the law.cornell.edu, the notes include live links to many documents and terms. This version does not include the links.

Source: https://www.law.cornell.edu/uscode/text/5/552a (October 2020)

References in Text

Section 552(e) of this title, referred to in subsec. (a)(1), was redesignated section 552(f) of this title by section 1802(b) of Pub. L. 99–570.

Section 6103 of the Internal Revenue Code of 1986, referred to in subsec. (a)(8)(B)(iv), (vii), is classified to section 6103 of Title 26, Internal Revenue Code.

Sections 404, 464, and 1137 of the Social Security Act, referred to in subsec. (a)(8)(B)(iv), are classified to sections 604, 664, and 1320b–7, respectively, of Title 42, The Public Health and Welfare.

The Achieving a Better Life Experience Act of 2014, referred to in subsec. (a)(8)(B)(x), probably means Pub. L. 113–295, div. B, Dec. 19, 2014, 128 Stat. 4056, known as the Stephen Beck, Jr., Achieving a Better Life Experience Act of 2014 or the Stephen Beck, Jr., ABLE Act of 2014. The Act does not contain a section 3.

For effective date of this section, referred to in subsecs. (k)(2), (5), (7), (l)(2), (3), and (m), see Effective Date note below.

Section 6 of the Privacy Act of 1974, referred to in subsec. (s)(1), is section 6 of Pub. L. 93–579, which was set out below and was repealed by section 6(c) of Pub. L. 100–503.

For classification of the Privacy Act of 1974, referred to in subsec. (s)(4), see Short Title note below.

The Consumer Financial Protection Act of 2010, referred to in subsec. (w), is title X of Pub. L. 111–203, July 21, 2010, 124 Stat. 1955, which enacted subchapter V (§ 5481 et seq.) of chapter 53 of Title 12, Banks and Banking, and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title note set out under section 5301 of Title 12 and Tables.

Codification

Section 552a of former Title 5, Executive Departments and Government Officers and Employees, was transferred to section 2244 of Title 7, Agriculture.

Amendments

2014—Subsec. (a)(8)(B)(x). Pub. L. 113–295 added cl. (x).

2010—Subsec. (a)(8)(B)(ix). Pub. L. 111–148 added cl. (ix).

Subsec. (w). Pub. L. 111–203 added subsec. (w).

2004—Subsec. (b)(10). Pub. L. 108–271 substituted "Government Accountability Office" for "General Accounting Office".

1999—Subsec. (a)(8)(B)(viii). Pub. L. 106–170 added cl. (viii).

1998—Subsec. (u)(6), (7). Pub. L. 105–362 redesignated par. (7) as (6), substituted "paragraph (3)(D)" for "paragraphs (3)(D) and (6)", and struck out former par. (6) which read as follows: "The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3)(D). Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and submission of a cost-benefit analysis and the reasons for granting the waiver."

1997—Subsec. (a)(8)(B)(vii). Pub. L. 105–34 added cl. (vii).

1996—Subsec. (a)(8)(B)(iv)(III). Pub. L. 104–193 substituted "section 404(e), 464," for "section 464".

Subsec. (a)(8)(B)(v) to (vii). Pub. L. 104–226 inserted "or" at end of cl. (v), struck out "or" at end of cl. (vi), and struck out cl. (vii) which read as follows: "matches performed pursuant to section 6103(l)(12) of the Internal Revenue Code of 1986 and section 1144 of the Social Security Act;".

Subsecs. (b)(12), (m)(2). Pub. L. 104–316 substituted "3711(e)" for "3711(f)".

1993—Subsec. (a)(8)(B)(vii). Pub. L. 103–66 added cl. (vii).

1990—Subsec. (p). Pub. L. 101–508 amended subsec. (p) generally, restating former pars. (1) and (3) as par. (1), adding provisions relating to Data Integrity Boards, and restating former pars. (2) and (4) as (2) and (3), respectively.

1988—Subsec. (a)(8) to (13). Pub. L. 100–503, § 5, added pars. (8) to (13).

Subsec. (e)(12). Pub. L. 100–503, § 3(a), added par. (12).

Subsec. (f). Pub. L. 100–503, § 7, substituted "biennially" for "annually" in last sentence.

Subsecs. (o) to (q). Pub. L. 100–503, § 2(2), added subsecs. (o) to (q). Former subsecs. (o) to (q) redesignated (r) to (t), respectively.

Subsec. (r). Pub. L. 100–503, § 3(b), inserted "and matching programs" in heading and amended text generally. Prior to amendment, text read as follows: "Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any

system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers."

Pub. L. 100–503, § 2(1), redesignated former subsec. (o) as (r).

Subsec. (s). Pub. L. 100–503, § 8, substituted "Biennial" for "Annual" in heading, "biennially submit" for "annually submit" in introductory provisions, "preceding 2 years" for "preceding year" in par. (1), and "such years" for "such year" in par. (2).

Pub. L. 100–503, § 2(1), redesignated former subsec. (p) as (s).

Subsec. (t). Pub. L. 100–503, § 2(1), redesignated former subsec. (q) as (t).

Subsec. (u). Pub. L. 100–503, § 4, added subsec. (u).

Subsec. (v). Pub. L. 100–503, § 6(a), added subsec. (v).

1984—Subsec. (b)(6). Pub. L. 98–497, § 107(g)(1), substituted "National Archives and Records Administration" for "National Archives of the United States", and "Archivist of the United States or the designee of the Archivist" for "Administrator of General Services or his designee".

Subsec. (l)(1). Pub. L. 98–497, § 107(g)(2), substituted "Archivist of the United States" for "Administrator of General Services" in two places.

Subsec. (q). Pub. L. 98–477 designated existing provisions as par. (1) and added par. (2).

1983—Subsec. (b)(12). Pub. L. 97–452 substituted "section 3711(f) of title 31" for "section 3(d) of the Federal Claims Collection Act of 1966 (31 U.S.C. 952(d))".

Subsec. (m)(2). Pub. L. 97–452 substituted "section 3711(f) of title 31" for "section 3(d) of the Federal Claims Collection Act of 1966 (31 U.S.C. 952(d))".

1982—Subsec. (b)(12). Pub. L. 97–365, § 2(a), added par. (12).

Subsec. (e)(4). Pub. L. 97–375, § 201(a), substituted "upon establishment or revision" for "at least annually" after "Federal Register".

Subsec. (m). Pub. L. 97–365, § 2(b), designated existing provisions as par. (1) and added par. (2).

Subsec. (p). Pub. L. 97–375, § 201(b), substituted provisions requiring annual submission of a report by the President to the Speaker of the House and President pro tempore of the Senate relating to the Director of the Office of Management and Budget, individual rights of access, changes or additions to systems of records, and other necessary or useful information, for provisions which had directed the President to submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the

reasons for the exemptions, and such other information as indicate efforts to administer fully this section.

1975—Subsec. (g)(5). Pub. L. 94–183 substituted "to September 27, 1975" for "to the effective date of this section".

Change of Name

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

Committee on Government Operations of House of Representatives treated as referring to Committee on Government Reform and Oversight of House of Representatives by section 1(a) of Pub. L. 104–14, set out as a note preceding section 21 of Title 2, The Congress. Committee on Government Reform and Oversight of House of Representatives changed to Committee on Government Reform of House of Representatives by House Resolution No. 5, One Hundred Sixth Congress, Jan. 6, 1999. Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019.

Effective Date of 2014 Amendment

Pub. L. 113–295, div. B, title I, § 102(f)(1), Dec. 19, 2014, 128 Stat. 4062, provided that: "The amendments made by this section [enacting section 529A of Title 26, Internal Revenue Code, and amending this section, section 5517 of Title 12, Banks and Banking, and sections 26, 877A, 4965, 4973, and 6693 of Title 26] shall apply to taxable years beginning after December 31, 2014."

Effective Date of 2010 Amendment

Pub. L. 111–203, title X, § 1082, July 21, 2010, 124 Stat. 2080, provided that the amendment made by section 1082 is effective on July 21, 2010.

Pub. L. 111–203, title X, § 1100H, July 21, 2010, 124 Stat. 2113, provided that: "Except as otherwise provided in this subtitle [subtitle H (§§ 1081–1100H) of title X of Pub. L. 111–203, see Tables for classification] and the amendments made by this subtitle, this subtitle and the amendments made by this subtitle, other than sections 1081 [amending section 8G of Pub. L. 95–452, set out in the Appendix to this title, and enacting provisions set out as a note under section 8G of Pub. L. 95–452] and 1082 [amending this section and enacting provisions set out as a note under this section], shall become effective on the designated transfer date."

[The term "designated transfer date" is defined in section 5481(9) of Title 12, Banks and Banking, as the date established under section 5582 of Title 12, which is July 21, 2011.]

Effective Date of 1999 Amendment

Amendment by Pub. L. 106–170 applicable to individuals whose period of confinement in an institution commences on or after the first day of the fourth month beginning after December 1999, see section 402(a)(4) of Pub. L. 106–170, set out as a note under section 402 of Title 42, The Public Health and Welfare.

Effective Date of 1997 Amendment

Amendment by Pub. L. 105–34 applicable to levies issued after Aug. 5, 1997, see section 1026(c) of Pub. L. 105–34, set out as a note under section 6103 of Title 26, Internal Revenue Code.

Effective Date of 1996 Amendment

Amendment by Pub. L. 104–193 effective July 1, 1997, with transition rules relating to State options to accelerate such date, rules relating to claims, actions, and proceedings commenced before such date, rules relating to closing out of accounts for terminated or substantially modified programs and continuance in office of Assistant Secretary for Family Support, and provisions relating to termination of entitlement under AFDC program, see section 116 of Pub. L. 104–193, as amended, set out as an Effective Date note under section 601 of Title 42, The Public Health and Welfare.

Effective Date of 1993 Amendment

Amendment by Pub. L. 103–66 effective Jan. 1, 1994, see section 13581(d) of Pub. L. 103–66, set out as a note under section 1395y of Title 42, The Public Health and Welfare.

Effective Date of 1988 Amendment

Pub. L. 100–503, § 10, Oct. 18, 1988, 102 Stat. 2514, as amended by Pub. L. 101–56, § 2, July 19, 1989, 103 Stat. 149, provided that:
"(a) In General.—
Except as provided in subsections (b) and (c), the amendments made by this Act [amending this section and repealing provisions set out as a note below] shall take effect 9 months after the date of enactment of this Act [Oct. 18, 1988].
"(b) Exceptions.—
The amendment made by sections 3(b), 6, 7, and 8 of this Act [amending this section and repealing provisions set out as a note below] shall take effect upon enactment.
"(c) Effective Date Delayed for Existing Programs.—In the case of any matching program (as defined in section 552a(a)(8) of title 5, United States Code, as added by section 5 of this Act) in operation before June 1, 1989, the amendments made by this Act (other than the amendments described in subsection (b)) shall take effect January 1, 1990, if—
"(1) such matching program is identified by an agency as being in operation before June 1, 1989; and
"(2) such identification is—
"(A) submitted by the agency to the Committee on Governmental Affairs of the Senate, the Committee on Government Operations of the House of Representatives, and the Office of Management and Budget before August 1, 1989, in a report which contains a schedule showing the dates on which the agency expects to have such matching program in compliance with the amendments made by this Act, and
"(B) published by the Office of Management and Budget in the Federal Register, before September 15, 1989."

Effective Date of 1984 Amendment

Amendment by Pub. L. 98–497 effective Apr. 1, 1985, see section 301 of Pub. L. 98–497, set out as a note under section 2102 of Title 44, Public Printing and Documents.
Effective Date

Pub. L. 93–579, § 8, Dec. 31, 1974, 88 Stat. 1910, provided that: "The provisions of this Act [enacting this section and provisions set out as notes under this section] shall be effective on and after the date of enactment [Dec. 31, 1974], except that the amendments made by sections 3 and 4 [enacting this section and amending analysis preceding section 500 of this title] shall become effective 270 days following the day on which this Act is enacted."

Short Title of 1990 Amendment

Pub. L. 101–508, title VII, § 7201(a), Nov. 5, 1990, 104 Stat. 1388–334, provided that: "This section [amending this section and enacting provisions set out as notes below] may be cited as the 'Computer Matching and Privacy Protection Amendments of 1990'."
Short Title of 1989 Amendment

Pub. L. 101–56, § 1, July 19, 1989, 103 Stat. 149, provided that: "This Act [amending section 10 of Pub. L. 100–503, set out as a note above] may be cited as the 'Computer Matching and Privacy Protection Act Amendments of 1989'."

Short Title of 1988 Amendment

Pub. L. 100–503, § 1, Oct. 18, 1988, 102 Stat. 2507, provided that: "This Act [amending this section, enacting provisions set out as notes above and below, and repealing provisions set out as a note below] may be cited as the 'Computer Matching and Privacy Protection Act of 1988'."
Short Title of 1974 Amendment

Pub. L. 93–579, § 1, Dec. 31, 1974, 88 Stat. 1896, provided: "That this Act [enacting this section and provisions set out as notes under this section] may be cited as the 'Privacy Act of 1974'."
Short Title

This section is popularly known as the "Privacy Act" and the "Privacy Act of 1974".

Termination of Reporting Requirements

For termination, effective May 15, 2000, of reporting provisions in subsec. (s) of this section, see section 3003 of Pub. L. 104–66, as amended, set out as a note under section 1113 of Title 31, Money and Finance, and page 31 of House Document No. 103–7.

Delegation of Functions

Functions of Director of Office of Management and Budget under this section delegated to Administrator for Office of Information and Regulatory Affairs by section 3 of Pub. L. 96–511, Dec. 11, 1980, 94 Stat. 2825, set out as a note under section 3503 of Title 44, Public Printing and Documents.

OMB Guidance on Electronic Consent and Access Forms

Pub. L. 116–50, § 3, Aug. 22, 2019, 133 Stat. 1073, provided that:
"(a) Guidance.—Not later than 1 year after the date of the enactment of this Act [Aug. 22, 2019], the Director shall issue guidance that does the following:
"(1) Requires each agency to accept electronic identity proofing and authentication processes for the purposes of allowing an individual to provide prior written consent for the disclosure of the individual's records under section 552a(b) of title 5, United States Code, or for individual access to records under section 552a(d) of such title.
"(2) Creates a template for electronic consent and access forms and requires each agency to post the template on the agency website and to accept the forms from any individual properly identity proofed and authenticated in accordance with paragraph (1) for the purpose of authorizing disclosure of the individual's records under section 552a(b) of title 5, United States Code, or for individual access to records under section 552a(d) of such title.
"(3) Requires each agency to accept the electronic consent and access forms described in paragraph (2) from any individual properly identity proofed and authenticated in accordance with paragraph (1) for the purpose of authorizing disclosure of the individual's records to another entity, including a congressional office, in accordance with section 552a(b) of title 5, United States Code, or for individual access to records under section 552a(d) [of such title].
"(b) Agency Compliance.—
Each agency shall comply with the guidance issued pursuant to subsection (a) not later than 1 year after the date on which such guidance is issued.
"(c) Definitions.—In this section:
"(1) Agency; individual; record.—
The terms 'agency', 'individual', and 'record' have the meanings given those terms in section 552a(a) of title 5, United States Code.
"(2) Director.—
The term 'Director' means the Director of the Office of Management and Budget."
Extension of Privacy Act Remedies to Citizens of Designated Countries

Pub. L. 114–126, Feb. 24, 2016, 130 Stat. 282, provided that:
"SECTION 1. SHORT TITLE.

"This Act may be cited as the 'Judicial Redress Act of 2015'.
"SEC. 2. EXTENSION OF PRIVACY ACT REMEDIES TO CITIZENS OF DESIGNATED COUNTRIES.
"(a) Civil Action; Civil Remedies.—With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under—
"(1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and
"(2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.
"(b) Exclusive Remedies.—
The remedies set forth in subsection (a) are the exclusive remedies available to a covered person under this section.
"(c) Application of the Privacy Act With Respect to a Covered Person.—

For purposes of a civil action described in subsection (a), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in paragraphs (1) and (2) of subsection (a).
"(d) Designation of Covered Country.—
"(1) In general.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a 'covered country' for purposes of this section if—
"(A)(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or
"(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information;
"(B) the country or regional economic integration organization, or member country of such organization, permits the transfer of personal data for commercial purposes between the territory of that country or regional economic organization and the territory of the United States, through an agreement with the United States or otherwise; and
"(C) the Attorney General has certified that the policies regarding the transfer of personal data for commercial purposes and related actions of the country or regional economic integration organization, or member country of such organization, do not materially impede the national security interests of the United States.
"(2) Removal of designation.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, revoke the designation of a foreign country or regional economic integration organization, or member country of such organization, as a 'covered country' if the Attorney General determines that such designated 'covered country'—
"(A) is not complying with the agreement described under paragraph (1)(A)(i);
"(B) no longer meets the requirements for designation under paragraph (1)(A)(ii);
"(C) fails to meet the requirements under paragraph (1)(B);
"(D) no longer meets the requirements for certification under paragraph (1)(C); or
"(E) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person.
"(e) Designation of Designated Federal Agency or Component.—
"(1) In general.—
The Attorney General shall determine whether an agency or component thereof is a 'designated Federal agency or component' for purposes of this section. The Attorney General shall not designate any agency or component thereof other than the Department of Justice or a component of the Department of Justice without the concurrence of the head of the relevant agency, or of the agency to which the component belongs.
"(2) Requirements for designation.—The Attorney General may determine that an agency or component of an agency is a 'designated Federal agency or component' for purposes of this section, if—
"(A) the Attorney General determines that information exchanged by such agency with a covered country is within the scope of an agreement referred to in subsection (d)(1)(A); or

"(B) with respect to a country or regional economic integration organization, or member country of such organization, that has been designated as a 'covered country' under subsection (d)(1)(B), the Attorney General determines that designating such agency or component thereof is in the law enforcement interests of the United States.
"(f) Federal Register Requirement; Nonreviewable Determination.—
The Attorney General shall publish each determination made under subsections (d) and (e). Such determination shall not be subject to judicial or administrative review.
"(g) Jurisdiction.—
The United States District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this section.
"(h) Definitions.—In this Act:
"(1) Agency.—
The term 'agency' has the meaning given that term in section 552(f) of title 5, United States Code.
"(2) Covered country.—
The term 'covered country' means a country or regional economic integration organization, or member country of such organization, designated in accordance with subsection (d).
"(3) Covered person.—
The term 'covered person' means a natural person (other than an individual) who is a citizen of a covered country.
"(4) Covered record.—The term 'covered record' has the same meaning for a covered person as a record has for an individual under section 552a of title 5, United States Code, once the covered record is transferred—
"(A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and
"(B) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.
"(5) Designated federal agency or component.—
The term 'designated Federal agency or component' means a Federal agency or component of an agency designated in accordance with subsection (e).
"(6) Individual.—
The term 'individual' has the meaning given that term in section 552a(a)(2) of title 5, United States Code.
"(i) Preservation of Privileges.—
Nothing in this section shall be construed to waive any applicable privilege or require the disclosure of classified information. Upon an agency's request, the district court shall review in camera and ex parte any submission by the agency in connection with this subsection.
"(j) Effective Date.—
This Act shall take effect 90 days after the date of the enactment of this Act [Feb. 24, 2016]."

Publication of Guidance Under Subsection (p)(1)(A)(ii)

Pub. L. 101–508, title VII, § 7201(b)(2), Nov. 5, 1990, 104 Stat. 1388–334, provided that: "Not later than 90 days after the date of the enactment of this Act [Nov. 5, 1990], the Director of the Office of Management and Budget shall publish guidance under subsection (p)(1)(A)(ii) of section 552a of title 5, United States Code, as amended by this Act."
Limitation on Application of Verification Requirement

Pub. L. 101–508, title VII, § 7201(c), Nov. 5, 1990, 104 Stat. 1388–335, provided that: "Section 552a(p)(1)(A)(ii)(II) of title 5, United States Code, as amended by section 2 [probably means section 7201(b)(1) of Pub. L. 101–508], shall not apply to a program referred to in paragraph (1), (2), or (4) of section 1137(b) of the Social Security Act (42 U.S.C. 1320b–7), until the earlier of—
"(1) the date on which the Data Integrity Board of the Federal agency which administers that program determines that there is not a high degree of confidence that information provided by that agency under Federal matching programs is accurate; or
"(2) 30 days after the date of publication of guidance under section 2(b) [probably means section 7201(b)(2) of Pub. L. 101–508, set out as a note above]."
Effective Date Delayed for Certain Education Benefits Computer Matching Programs

Pub. L. 101–366, title II, § 206(d), Aug. 15, 1990, 104 Stat. 442, provided that:
"(1) In the case of computer matching programs between the Department of Veterans Affairs and the Department of Defense in the administration of education benefits programs under chapters 30 and 32 of title 38 and chapter 106 of title 10, United States Code, the amendments made to section 552a of title 5, United States Code, by the Computer Matching and Privacy Protection Act of 1988 [Pub. L. 100–503] (other than the amendments made by section 10(b) of that Act) [see Effective Date of 1988 Amendment note above] shall take effect on October 1, 1990.
"(2) For purposes of this subsection, the term 'matching program' has the same meaning provided in section 552a(a)(8) of title 5, United States Code."

Implementation Guidance for 1988 Amendments

Pub. L. 100–503, § 6(b), Oct. 18, 1988, 102 Stat. 2513, required the Director, pursuant to section 552a(v) of this title, to develop guidelines and regulations for the use of agencies in implementing amendments made by Pub. L. 100–503 not later than 8 months after Oct. 18, 1988.

Construction of 1988 Amendments

Pub. L. 100–503, § 9, Oct. 18, 1988, 102 Stat. 2514, provided that: "Nothing in the amendments made by this Act [amending this section and repealing provisions set out as a note below] shall be construed to authorize—
"(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;
"(2) the direct linking of computerized systems of records maintained by Federal agencies;
"(3) the computer matching of records not otherwise authorized by law; or
"(4) the disclosure of records for computer matching except to a Federal, State, or local agency."

Congressional Findings and Statement of Purpose

Pub. L. 93–579, § 2, Dec. 31, 1974, 88 Stat. 1896, provided that:
"(a) The Congress finds that—
"(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;
"(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
"(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

"(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
"(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.
"(b) The purpose of this Act [enacting this section and provisions set out as notes under this section] is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—
"(1) permit an individual to determine what rec-ords pertaining to him are collected, maintained, used, or disseminated by such agencies;
"(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
"(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
"(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
"(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
"(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act."

Privacy Protection Study Commission

Pub. L. 93–579, § 5, Dec. 31, 1974, 88 Stat. 1905, as amended by Pub. L. 95–38, June 1, 1977, 91 Stat. 179, which established the Privacy Protection Study Commission and provided that the Commission study data banks, automated data processing programs and information systems of governmental, regional and private organizations to determine standards and procedures in force for protection of personal information, that the Commission report to the President and Congress the extent to which requirements and principles of section 552a of title 5 should be applied to the information practices of those organizations, and that it make other legislative recommendations to protect the privacy of individuals while meeting the legitimate informational needs of government and society, ceased to exist on September 30, 1977, pursuant to section 5(g) of Pub. L. 93–579.

Guidelines and Regulations for Maintenance of Privacy and Protection of Records of Individuals

Pub. L. 93–579, § 6, Dec. 31, 1974, 88 Stat. 1909, which provided that the Office of Management and Budget shall develop guidelines and regulations for use of agencies in implementing provisions of this section and provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies, was repealed by Pub. L. 100–503, § 6(c), Oct. 18, 1988, 102 Stat. 2513.

Disclosure of Social Security Number

Pub. L. 93–579, § 7, Dec. 31, 1974, 88 Stat. 1909, provided that:
"(a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

"(2) the [The] provisions of paragraph (1) of this subsection shall not apply with respect to—
"(A) any disclosure which is required by Federal statute, or
"(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.
"(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."

Authorization of Appropriations to Privacy Protection Study Commission

Pub. L. 93–579, § 9, Dec. 31, 1974, 88 Stat. 1910, as amended by Pub. L. 94–394, Sept. 3, 1976, 90 Stat. 1198, authorized appropriations for the period beginning July 1, 1975, and ending on September 30, 1977.

Ex. Ord. No. 9397. Numbering System for Federal Accounts Relating to Individual Persons

Ex. Ord. No. 9397, Nov. 22, 1943, 8 F.R. 16095, as amended by Ex. Ord. No. 13478, § 2, Nov. 18, 2008, 73 F.R. 70239, provided:

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and

WHEREAS some seventy million persons have heretofore been assigned account numbers pursuant to the Social Security Act; and

WHEREAS a large percentage of Federal employees have already been assigned account numbers pursuant to the Social Security Act; and

WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single, unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems:

NOW, THEREFORE, by virtue of the authority vested in me as President of the United States, it is hereby ordered as follows:

1. Hereafter any Federal department, establishment, or agency may, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to title 20, section 422.103 of the Code of Federal Regulations and pursuant to paragraph 2 of this order.

2. The Social Security Administration shall provide for the assignment of an account number to each person who is required by any Federal agency to have such a number but who has not previously been assigned such number by the Administration. The Administration may accomplish this purpose by (a) assigning such numbers to individual persons, (b) assigning blocks of numbers to Federal agencies for reassignment to individual persons, or (c) making such other arrangements for the assignment of numbers as it may deem appropriate.

3. The Social Security Administration shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an account or the name and other identifying data pertaining to any account number of any such person.

4. The Social Security Administration and each Federal agency shall maintain the confidential character of information relating to individual persons obtained pursuant to the provisions of this order.

5. There shall be transferred to the Social Security Administration, from time to time, such amounts as the Director of the Office of Management and Budget shall determine to be required for reimbursement by any Federal agency for the services rendered by the Administration pursuant to the provisions of this order.

6. This order shall be implemented in accordance with applicable law and subject to the availability of appropriations.

7. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

8. This order shall be published in the Federal Register.

Classified National Security Information

For provisions relating to a response to a request for information under this section when the fact of its existence or nonexistence is itself classified or when it was originally classified by another agency, see Ex. Ord. No. 13526, § 3.6, Dec. 29, 2009, 75 F.R. 718, set out as a note under section 3161 of Title 50, War and National Defense.

*****