September 16, 2015

Representative Bob Goodlatte, Chairman,
Representative John Conyers, Jr., Ranking Member
U.S. House of Representatives Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Re: Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015

Dear Chairman Goodlatte and Rep. Conyers:

We are writing to you regarding H.R. 1428, the Judicial Redress Act of 2015. We are aware that the House Judiciary Committee has scheduled a markup of H.R. 1428 this week,[1] following the recent announcement of an E.U.-U.S. data transfer agreement.[2]

EPIC appreciates your interest in this important issue. Data protection remains a key concern for transatlantic data transfers. Your bill seeks to extend certain Privacy Act safeguards to non-U.S. persons, but we do not believe it provides adequate protection to permit data transfers. Moreover, as you are considering amendments to the Privacy Act, we urge you to include several other recommendations to modernize the Act that EPIC and members of Congress have recently proposed.

EPIC is an independent, non-profit research organization in Washington, D.C. that frequently advises Congress and the courts about emerging privacy and civil liberties issues. At the request of members of Congress, EPIC has previously made recommendations regarding Privacy Act modernization.[3] EPIC routinely provides comments to federal agencies regarding Privacy Act compliance, and we have provided *amicus* briefs to the U.S. Supreme Court in two Privacy Act cases.[4] Moreover, we are very familiar with the data protection concerns arising from the transfer of personal information between the European Union and the United States.[5]

---

[1] *Markup of: H.R. 1428, The "Judicial Redress Act of 2015,"* U.S. H. R. Comm. on the Judiciary (Sept. 17, 2015), http://judiciary.house.gov/index.cfm/markups-meetings?ID=9CB82F32-81A1-472E-B94E-408772DE7031.

[2] *EU-US Data Transfer Agreement*, EPIC (2015), https://epic.org/privacy/intl/data-agreement/index.html.

[3] *See, e.g.*, Letter from Marc Rotenberg, EPIC Executive Director, Khaliah Barnes, EPIC Open Government Fellow, & Alan Butler, EPIC Appellate Advocacy Fellow, to Senator Daniel Akaka, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (May 14, 2012), *available at* https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf; Letter from Marc Rotenberg, EPIC Executive Director, & Khaliah Barnes, EPIC Open Government Fellow, to Senator Daniel Akaka, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (Mar. 27, 2012), *available at* https://epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf.

[4] Br. EPIC as *Amici Curiae* Supporting Petitioners, *Doe v. Chao*, 540 U.S. 614 (2014) (No. 02-1377), *available at* https://epic.org/privacy/chao/Doe_amicus.pdf; Br. EPIC as *Amicus Curiae* Supporting

This statement identifies concerns in the current draft of H.R. 1428 and proposes specific changes.

I. The Privacy Act Fix for EU-U.S. Data Transfers is Simple

The Judicial Redress Act of 2015 arises from the concern that personal information transferred from the European Union to the United States lacks adequate privacy protection. That is because the Privacy Act, as adopted in 1974, defined an "individual" entitled to protection under the Act as "a citizen of the United States or an alien lawfully admitted for permanent residence.[6] The definition reflected the reality of the time, which was that there was little information about non-U.S. persons maintained by U.S. federal agencies.

Most U.S. privacy laws that were enacted subsequent to the Privacy Act of 1974 do not maintain this distinction.[7] Moreover, U.S. federal agencies have routinely made extensive demands on European companies and European government agencies for the personal information of European citizens. The request that the U.S. Privacy Act be updated to reflect the fact that personal data on E.U. citizens is now routinely stored by U.S. federal agencies followed directly from the practices initiated by U.S. agencies.

The simple legislative solution to the problem of updating the application of the Privacy Act for non-U.S. persons would be amend the definition of an "individual" as follows:

(2) the term "individual" means any natural person;

This definition would update the Privacy Act to reflect current federal agency recordkeeping practices. It is the most straightforward solution for permitting transborder data flows. It also mirrors the approach of the U.S. Freedom of Information Act, which does not distinguish between U.S. and non-U.S. persons.[8]

Respondent, *FAA v. Cooper*, 132 S.Ct. 1441 (2012) (No. 10–1024), *available at* https://epic.org/amicus/cooper/Cooper-EPIC-Brief.pdf.

[5] *See, e.g.*, Marc Rotenberg, *On International Privacy: A Path Forward for the US and Europe*, Harv. Int'l Rev. (June 2014), http://hir.harvard.edu/archives/5815; Marc Rotenberg & David Jacobs, Updating the Law of Information Privacy: The New Framework of the European Union, 36 Harv. J.L. & Pub. Policy 605 (2013).

[6] 5 U.S.C. § 552a(a)(2). *See generally, The Privacy Act 1974*, EPIC (2015), https://epic.org/privacy/1974act/.

[7] *See, e.g.*, 15 U.S.C. § 1681a(c) (West 2015) (stating that the definition of "consumer" for purposes of the Fair Credit Reporting Act "means an individual"); 15 U.S.C. § 1692a(3) (West 2015) (stating that the definition of "consumer" for purposes of the Fair Debt Collection Practices Act "means any natural person obligated or allegedly obligated to pay any debt"); 18 U.S.C. § 2721(a)(1) (West 2015) (prohibiting under the Driver's Privacy Protection Act the disclosure of personal information about "any individual" in connection with a motor vehicle record).

[8] 5 U.S.C. § 552(a)(3)(A).

In the alternative, if the approach of H.R. 1428 is to be maintained, EPIC proposes specific changes that would satisfy the stated purpose of the bill, which is to "extend Privacy Act remedies to citizens of certified states, and for other purposes."[9]

A. The Judicial Redress Act Should Provide the Same Basis for Legal Actions for Non-U.S Persons as it Does for U.S. Persons

The Privacy Act currently provides four causes of action: (1) an agency's failure to amend a U.S. person's record upon her request;[10] (2) an agency's refusal to comply with a U.S. person's request for access to her records;[11] (3) an agency's failure to maintain her records with the accuracy, relevance, timeliness, and completeness necessary for a fair adjudication of rights or benefits and the agency subsequently makes an adverse decision;[12] and (4) an agency's failure to comply with any other provision of the Privacy Act or any relevant promulgated regulations.[13]

The Judicial Redress Act, as currently drafted, provides only limited opportunities for non-U.S. persons to seek redress under the Privacy Act. First, it limits the scope of the Privacy Act's catchall provision, § 552a(g)(1)(D), to only intentional or willful violations of § 552a(b), which prohibits disclosure of personal information without consent unless the disclosure is subject to the enumerated exceptions.[14] Under the bill, non-U.S. persons will not be able to sue agencies for failure to comply with any other provision of the Privacy Act, nor will they be able to sue for an agency's violation of its own regulations. In addition, a non-U.S. person will only be able to sue a "designated agency" for improper disclosure of her personal information.[15]

Second, the bill substantially limits a non-U.S. person's ability to sue an agency for failure to amend a record or refusal to provide access to a record.[16] According to H.R. 1428, non-U.S. persons will only be able to sue "designated agencies" for refusal to provide access to or for failure to amend a record.[17] Federal agencies that are not "designated agencies" but which maintain records on non-U.S. persons fall outside the scope of the Act's provisions.

Finally, non-U.S. persons have no ground to challenge an agency for an adverse decision—such as a denial of a visa or refugee resettlement application—when the adverse decision resulted from the agency's failure to maintain their records with the requisite accuracy, relevance, timeliness, and completeness necessary for fair determinations.[18]

---

[9] H.R. 1428 Preamble.
[10] 5 U.S.C. § 552a(g)(1)(A).
[11] *Id.* § 552a(g)(1)(B).
[12] *Id.* § 552a(g)(1)(C).
[13] *Id.* § 552a(g)(1)(D).
[14] H.R. 1428(a)(1).
[15] Although H.R. 1428(a)(1) does not explicitly limit itself to "designated agencies" as defined in the bill, subsection(a) applies only to "covered records." As defined later in the bill, "covered records" are *only* information that is transferred *to* a designated federal agency or component. H.R. 1428(h)(4). Therefore, a non-U.S. person can only sue a designated agency for improper disclosure in violation of § 552a(b).
[16] 5 U.S.C. § 552a(g)(1)(A) and (B).
[17] H.R. 1428(a)(2).
[18] 5 U.S.C. § 552a(g)(1)(C).

Recommendation

To the extent that federal agencies maintain personal information on non-U.S. persons, EPIC recommends that the Judicial Redress Act grant all such persons the same right of judicial redress currently available to U.S. persons under § 552a(g). The Privacy Act already contains many exceptions that allow an agency to withhold the release of sensitive information as necessary.[19]

B. The Judicial Redress Act Should Apply Privacy Act Obligations to All Federal Agencies

The Privacy Act applies to all agencies of the U.S. Government, including all executive departments, military departments, Government corporations, Government-controlled corporations, independent regulatory agencies, or other establishments in the executive branch.[20]

H.R. 1428, by contrast, limits the number of agencies subject to judicial redress by non-U.S. persons. A non-U.S. person can only sue "designated agencies" for willful or intentional improper disclosure of records, the refusal to provide access to records, or for failure to grant a request to amend records.[21] Under H.R. 1428, the U.S. Attorney General—with the concurrence of any agency head beyond the Department of Justice—has complete discretion to designate a federal agency or component as subject to the Privacy Act's access and amendment requirements.[22] Moreover, H.R. 1428 strips such determinations, if and when they are made, from any judicial or administrative review.[23] This provision extends substantial and unbounded discretion to members of the Executive Branch to select the U.S. agencies that will have to comply with the Privacy Act.

Recommendation

EPIC recommends that H.R. 1428 require all agencies—consistent with the meaning of "agency" in § 552a(a)(1) and subject to the same exemptions in § 552a(j) and § 552a(k)—to comply with the Privacy Act when maintaining records about non-U.S. persons.

---

[19] *Id.* § 552a(j), (k).
[20] 5 U.S.C. § 552(f). *See* § 552a(1).
[21] H.R. 1428(a). As clarified above, although H.R. 1428(a)(1) does not explicitly limit itself to "designated agencies" as defined in the bill, subsection(a) applies only to "covered records." As defined later in the bill, "covered records" are *only* information that is transferred *to* a designated federal agency or component. H.R. 1428(h)(4). Therefore, a non-U.S. person can only sue a designated agency for improper disclosure in violation of § 552a(b).
[22] H.R. 1428(e).
[23] H.R. 1428(f).

C. The Judicial Redress Act Should Extend Privacy Act Protections to All Non-U.S. Persons

The Privacy Act applies to the records of all U.S. persons, defined as U.S. citizens or aliens lawfully admitted to the U.S. for permanent residence.[24]

H.R. 1428, by contrast, extends limited Privacy Act protections to a subset of non-U.S. persons who are citizens of "covered countries." Under H.R. 1428, a covered country is designated at the discretion of the U.S. Attorney General, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security.[25] As with the "designated agencies," H.R. 1428 strips determinations of covered countries, if and when they are made, from any judicial or administrative review.[26] This provision extends substantial and unbounded discretion to members of the Executive Branch to select which non-U.S. persons will enjoy already limited protections under the Privacy Act.

In addition, non-U.S. persons may receive protections under the Privacy Act if their country first "effectively shares information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses."[27] In effect, some non-U.S. persons will not be eligible for protection under the Privacy Act until the country of their citizenship first transfers information to the United States. This provision turns privacy protections on their head, requiring data transfer *before* privacy protections are established.

The U.S. Attorney General, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, has complete discretion to remove a covered country from its designation.[28] The bill, however, makes no mention as to what will happen to the non-U.S. persons' data when their country loses covered status.

Finally, the Executive Branch can strip a covered country of its designation if, among other reasons, it "impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person."[29] This provision suggests that a country could be stripped of its covered status for demanding that a private entity within its borders comply with that country's privacy or data sharing laws. This is contrary to the explicit carve-out in the GATT and other trade agreements.[30]

[24] 5 U.S.C. § 552a(a)(2).
[25] H.R. 1428(d).
[26] H.R. 1428(f).
[27] H.R. 1428(d)(1)(B).
[28] H.R. 1428(d)(2).
[29] H.R. 1428(d)(2)(C).
[30] General Agreement on Tariffs and Trade, Oct.30, 1947, 61 Stat. A-11, 55 U.N.T.S.194 (holding member states's actions "[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services . . . .").

Recommendation

EPIC recommends the complete removal of subsection (d)(2)(C), which improperly hinges a person's privacy rights on a government's willingness to ignore its own data protection laws for private entities operating within its own borders.

EPIC also recommends that Congress avoid *ad hoc* determinations by the Executive branch regarding the scope of Privacy Act enforcement. The simple solution proposed by EPIC at the outset would avoid this problem. At a minimum, the Judicial Redress Act should extend non-revocable legal rights to citizens of all countries subject to the E.U.-U.S. Umbrella Agreement and other similar agreements that may be adopted in the future.

D. The Judicial Redress Act Should Apply to All Records Maintained by Federal Agencies

The Privacy Act applies to a broad category of records, defined as "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."[31] In other words, the Privacy Act applies to all personal information maintained by the agency, regardless of the source or the content.

The Judicial Redress extends Privacy Act protections to only a limited subset of records maintained by federal agencies. Under the bill, personal information only falls within the Privacy Act if a public authority or private entity within a covered country has transferred it to a designated federal agency or component.[32] In other words, only records received by the United States from the covered country will receive Privacy Act protections; other non-U.S. person records received from other countries or otherwise obtained by the relevant agency will remain unprotected. This is clearly contrary to the purpose and structure of the Privacy Act, which is to enable individuals to determine what personal information, obtained from any source, is maintained by a federal agency.

Recommendation

EPIC recommends that H.R. 1428 apply to all records acquired by agencies (as defined in the Privacy Act), regardless of the source of the record.

II. Additional Recommendations for Privacy Act Modernization

EPIC further recommends that the Committee take this opportunity to enact other amendments to the Privacy Act. Given increased public concern about government data security, a recent decision of the Supreme Court, and the OPM breach, Congressional action to strengthen

[31] 5. U.S.C. § 552a(a)(4).
[32] H.R. 1428(h)(4).

the Privacy Act of 1974 is long overdue. These recommendations follow from similar proposals by Senator Akaka (D-HI) in S. 1732.[33]

A. Congress Should Establish a Privacy Agency to Enforce the Privacy Act

The Privacy Act should be amended to create an independent privacy agency, as Congress contemplated in 1974 when it enacted the Privacy Act.[34] EPIC has previously recommended the establishment of a privacy agency to ensure independent enforcement of the Privacy Act, develop additional recommendations for privacy protection, and provide permanent leadership within the federal government on this important issue. [35]

The enforcement of the Privacy Act is the cornerstone of the E.U.-U.S. Umbrella Agreement. But the current enforcement mechanism for the Privacy Act is inadequate. The Judicial Redress Act provides an opportunity to create the federal privacy agency that Congress contemplated when it passed the Privacy Act.

B. Congress Should Provide Relief for Nonpecuniary Privacy Harms

Contrary to the views of many experts and the legislative history, the Supreme Court recently determined that the Privacy Act "does not unequivocally authorize an award of damages for mental or emotional distress."[36] The 5-3 opinion was highly controversial. Writing in dissent, Justice Sotomayor, joined by Justices Ginsburg and Breyer, explained that the holding was contrary to Supreme Court precedent and the common sense understanding that "the primary, and often only, damages sustained as a result of an invasion of privacy [are] namely mental or emotional distress."[37] These Justices said that the Privacy Act's "core purpose [is] redressing and deterring violations of privacy interests."[38]

The warning of the dissenters in *Cooper* has proved prescient. In the absence of strong incentives to safeguard personal information, federal agencies have experienced massive data breaches threatening not only the economic but also non-economic interests of individuals.[39]

---

[33] Privacy Act Modernization for the Information Age Act of 2011, S. 1732, 112th Cong.§ 552a(g)(4).
[34] Staff of S. Comm. on Gov't Operations, 93d Cong., Materials Pertaining to S. 3418 and Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information (Comm. Print 1974) (collecting materials on S. 3418, a bill to establish a Federal Privacy Board).
[35] *See, e.g.*, Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 *Gov't Info. Q.* 79 (1991); *Communications Privacy: Hearing Before the Subcomm. on Courts and Intellectual Prop. of H. Comm. on the Judiciary*, 105th Cong. (1998) (testimony of Marc Rotenberg), *available at* https://www.epic.org/privacy/internet/rotenberg-testimony-398.html.
[36] *FAA v. Cooper*, 132 S. Ct. 1441, 1456 (2012).
[37] *Id*.
[38] *Id*. at 1456, 1462.
[39] *Recent Data Breaches Illustrate Need for Strong Controls Across Federal Agencies: Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Sec. Tech., of the H. Comm. on Homeland Sec.*, 114th Cong. (2015) (Statement of Gregory C. Wilshusen, Director, Information Security Issues, Gov't Accountability Office).

Congress has held many hearings this year on the enormous risks now facing Americans because of failure to update and enforce the Privacy Act.[40]

In light of the OPM data breach, the Judicial Redress Act should make clear that individuals may be compensated for provable, nonpecuniary harms arising from violations of the Act.

C. Congress Should Address Concerns Over Access to Records

A key goal for the Privacy Act was to establish standards for the data the government collects about individuals. In passing the Act, Congress found that "the opportunities for an individual to secure employment, insurance, and credit, and his rights to due process, and other legal protections are endangered by the misuse of certain information systems," and therefore "it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies."[41] To that end, Congress passed the Act to ensure, among other things, that any information held by the government would be "current and accurate for its intended use."[42]

Without meaningful access to records and the ability to contest their accuracy, individuals may be unaware of records accuracy problems. However, many agencies currently exempt themselves from access obligations. For example, the Federal Bureau of Investigation has relied on 5 U.S.C. § 552a(j)(2) to dispense with its statutory duty to ensure the accuracy and completeness of the over 39 million criminal records it maintains in its National Crime Information Center (NCIC) database.[43] Circumventing that statutory obligation poses significant risks not only for individuals whose record files may be part of this data system, but also for communities that rely on law enforcement records to employ effective, reliable tools for ensuring public safety.

EPIC recommends that Congress strengthen the access and accuracy requirements of the Privacy Act and limit the exemptions agencies can claim. Such measures are necessary to hold agencies accountable for the accuracy of their systems of records, rather than allowing them to easily exempt themselves of this important duty.

---

[40] See, e.g., The IRS Data Breach: Steps to Protect Americans' Personal Information: Before the S. Comm. Homeland Sec. and Gov't Affairs, 114th Cong. (2015); Under Attack: Federal Cybersecurity and the OPM Data Breach: Before the S. Comm. Homeland Sec. and Gov't Affairs, 114th Cong. (2015); OPM: Data Breach: Hearing Before the H. Comm. on Oversight and Gov't Reform, 114th Cong. (2015).
[41] Congressional Findings and Statement of Purpose, Pub. L. No. 93-579, §2(a)(3) & (5) (1974).
[42] Congressional Findings and Statement of Purpose, Pub. L. No. 93-579, §2(b)(4)(1974).
[43] *See* 28 CFR § 16.96(g)–(h).

D. Congress Should Amend the Privacy Act Definition of "Routine Use" to Prevent Unwarranted Disclosure of Individual Records and Preserve the Legislative Intent of the Act

The legislative history of the Privacy Act indicates that the "routine use" for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> The [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[44]

Agencies are already in the practice of establishing overly broad purposes under which they are permitted to collect and disclose records on individuals. Oftentimes in a tautological fashion, agencies will state in their Federal Record systems of records notice that the purpose for maintaining and collecting records is to collect and maintain records on a certain group of individuals.[45]

To prevent agencies from claiming broad-based routine use disclosure exemptions, EPIC proposes the following language for 5 U.S.C. § 552(a)(7):

> (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. Under this provision, the purpose for which the agency collects information cannot be "to collect information and/or records."

Clarifying the definition in this manner would aid in preventing unwarranted disclosure of individual records, and is true to the Privacy Act's legislative intent.

[44] Staff. of Joint Comm., 94th. Cong., Rep. on Legislative History of the Privacy Act of 1974 S. 3418 (Pub. L. No. 93-579)1031 (Comm. Print 1976).

[45] *See, e.g.,* Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP-001, Import Information System, System of Records, 80 Fed. Reg. 49256 (proposed Aug. 17, 2015); Implementation of the Privacy Act of 1974, as Amended; New System of Records Notice, Digital Identity Access Management System, 79 Fed. Reg. 58372 (proposed Sept. 29, 2014);
Privacy Act of 1974; Department of Homeland Security/United States Secret Service – 003 Non-Criminal Investigation Information System of Records, 76 Fed. Reg. 66937 (proposed Oct. 28, 2011)

E. The Privacy Act Should Be Amended to Require Federal Agencies to Evaluate and Consider Public Comments on Proposed System or Records Before the Systems Take Effect

The Privacy Act requires federal agencies to publish notice of their systems of records in the Federal Register. The current Privacy Act provision governing agency Federal Register requirements, 5 U.S.C. § 552a(e)(11), states:

> (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

At present, agencies are not required under the Privacy Act to respond to comments received in response to systems of records notices. More troublingly, the Privacy Act does not prohibit agencies from making their systems of records go into effect on the same day that comments are due. These failures result in a lack of meaningful agency accountability to the public and effectively defeat the current Privacy Act system of records public comment opportunity.

Conclusion

Because the Committee markup on H.R. 1428 was scheduled without a public hearing, EPIC reserves the right to supplement this statement. EPIC further welcomes the opportunity to testify or provide additional information to the Committee.

We appreciate your consideration of our views.

Sincerely,

Marc Rotenberg
President and Executive Director
EPIC

John Tran
EPIC Open Government Counsel

Claire Gartland
EPIC Consumer Law Fellow

Fanny Hidvegi
EPIC International Law Fellow

Aimee Thomson
EPIC Appellate Advocacy Fellow