

July 8, 2022

The CASES Act: Implementation and Issues for Congress

The CASES Act is intended to modernize and simplify what has been an inconsistent and variable process of obtaining an individual's written consent for information disclosure. The act would enable constituents to provide electronic authorization to additional parties, such as Members of Congress and their offices, to resolve constituent inquiries, compared to the current range of requirements for verbal or email authorizations, or "wet" signatures.

The Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, or the CASES Act (P.L. 116-50), is designed to improve access to, and the efficiency of, government services and agencies for constituents by updating the casework process for an increasingly digital environment. Processing casework information often requires the disclosure of the constituent's individually identifiable information to a congressional office, and is subject to disclosure restrictions under the Privacy Act of 1974 (5 U.S.C. 552a). Generally, the Privacy Act prohibits disclosure of individually identifiable information by federal agencies to third parties, including congressional offices, without written consent.

The CASES Act requires the Office Management and Budget (OMB) to issue guidance requiring agencies to

- accept electronic identity proofing and authentication processes;
- create a template for electronic consent and access forms and require posting of the templates on agency websites; and
- require each agency to accept electronic consent and access forms.

Agencies were required by November 21, 2021, to comply with OMB implementation guidance, contained in Memorandum M-21-04. Most agencies are still in the process of putting procedures in place, however.

Congressional Casework and Privacy

Most Members of Congress routinely solicit and respond to requests from constituents for assistance with federal agencies. In general, agencies cannot reply to a congressional inquiry without a Privacy Act release form signed by the constituent requesting assistance. The form authorizes the Member to access a constituent's individually identifiable information to assist in the resolution of a case, and prevents the unauthorized disclosure of individually identifying information. For more information on casework, see CRS Report RL33209,

Casework in a Congressional Office: Background, Rules, Laws, and Resources.

The process of manually obtaining a signed authorization and transmitting the form to an agency has been a time-consuming process for both constituents and caseworkers, which sometimes delays consideration of the case by an agency. In addition, agencies across the federal government have required different versions of privacy release forms specific to their agencies. Some agencies have accepted electronic versions of privacy authorizations from congressional offices in a variety of formats, despite lacking clear authorization to do so. This has raised casework management concerns in some congressional offices.

The Privacy Act of 1974

The Privacy Act governs the disclosure of government information collected about individuals. Generally, the statute establishes agency processes to determine lawful uses of individually identifiable information and protect against unauthorized disclosure of the information. For more information about the Privacy Act, see CRS Report R47058, *Access to Government Information: An Overview. The Privacy Act*

- allows citizens of the United States or aliens lawfully admitted for permanent residence to access and correct information collected on them by federal agencies;
- restricts how and when these records may be shared to third parties without an individual's written consent; and
- allows agencies to share information on individuals for select purposes without requiring the written consent of the individual (5 U.S.C. 552a(b)).

OMB has interpreted the Privacy Act's concept of individually identifiable information as *personally identifiable information* (PII). OMB defines PII in Memorandum M-07-16 as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc...." Under statute, PII may only be shared with an entity that has been designated by the individual. (In some cases, it may be shared without the individual's written consent under one of the Privacy Act's 12 exceptions described in 5 U.S.C. 552a(b).)

Implementation and Oversight

Under Memorandum M-21-04, agencies are required to provide a digital service option to individuals requesting access to their records or consenting to their disclosure. They were also required to accept properly identity-proofed

and authenticated electronic access and consent forms by November 2021. In addition, agencies must develop digital privacy release form templates consistent with those provided by OMB.

Implementation of these requirements must conform to OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access*, and National Institute of Standards and Technology (NIST) Special Publication 800-63, *Digital Identity Guidelines*. Under these guidelines, agencies select the appropriate level of identity authentication based on the risks to the individual of unauthorized disclosure of the information. Because these levels of identity authentication require different levels of documentation and verification, agency decisions under these guidelines may vary despite the CASES Act's intent to simplify and expedite the process for constituents and caseworkers.

Congressional Oversight

On January 12, 2022, Representatives Gerald E. Connolly and Jody Hice, chair and ranking member of the Subcommittee on Government Operations of the House Committee on Oversight and Reform, sent joint letters requesting information about the implementation of the CASES Act. The letters were sent to the heads of five federal agencies that frequently interact with congressional offices regarding constituent service issues. These agencies are the Department of Veterans Affairs (VA); Internal Revenue Service (IRS); United States Citizenship and Immigration Services (USCIS); Social Security Administration (SSA); and Centers for Medicare and Medicaid Services (CMS). CRS has not identified any response from the agencies to the letters.

Improving Constituent Services

Through passage of the CASES Act, Congress sought to improve access and efficiency of government services by modernizing the process of accessing individually identifiable information for constituents. The law might afford agencies with opportunities to use evolving technologies to manage inquiries from, and correspondence with, congressional offices and constituents. However, questions remain about whether implementation of the law can fully streamline the constituent's experience with the federal government.

Interaction with Other Privacy Policies

The CASES Act authorizes the electronic release of information protected by the Privacy Act for some constituent service matters. It does not appear to provide similar processes to authorize electronic release of protected information pursuant to other privacy provisions. These include the Health Insurance Portability and Accountability Act (HIPAA), which provides in part for the protection of individuals' healthcare information, or USCIS and other Department of Homeland Security entities' protection of information related to immigration cases. As the CASES Act is implemented by executive agencies, Congress might consider legislative and oversight options for expanding the scope of electronic authorizations to incorporate other privacy policies.

Oversight of the Routine Use Exception

Subject to the Privacy Act's written consent requirement, information on an individual may be shared with other persons, such as congressional caseworkers or government agencies. However, the Privacy Act also provides 12 exceptions to the written consent requirement from individuals, raising questions about the intended use of these exceptions by government agencies. One of these exceptions is the "routine use" exception, which was designed to allow individually identifiable information disclosures for purposes compatible with the original information collection.

As described by the Department of Justice in its 2020 *Overview of the Privacy Act of 1974*,

Courts have generally held that routine use disclosures to process an individual's application for a benefit, program participation, or a position are "compatible" disclosures under the routine use disclosure exception.

This interpretation could expedite decisions related to constituent casework, depending on the judgment of the agency. Conversely, the routine use exception has also been generally interpreted to permit disclosures to further investigations.

Agency and court interpretations of the routine use exception may both help and hinder congressional casework. However, the application of routine use to benefits and program administration may warrant congressional interest. Congress, in its oversight efforts, may consider directing agencies to proactively review their interpretation of compatible routine uses to make agencies more responsive and to improve constituent interactions with the federal government.

Continuing Digital Skills, Access Gaps

As electronic authorizations become more routine, a potential concern is the issue of varying access to computers and the skills to operate them among some constituents who might seek assistance from their Members. This could present workload management challenges in some Member offices if constituents seek help from casework staff to complete electronic authorizations. Constituents, Member offices, Congress, and executive agencies might not be able to take advantage of the full potential benefits of electronic authorizations in these circumstances. Individual Member offices might consider instituting office policies related to electronic authorization processes. More broadly, Congress might consider how to address constituent service concerns as part of broader policies meant to address and reduce disparities in access to technology and the skills to use those resources.

Meghan M. Stuessy, Analyst in Government Organization and Management

R. Eric Petersen, Specialist in American National Government

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.