epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

General Services Administration

on

Notice of a Modified System of Records: *Login.gov*

87 Fed. Reg. 70,819

December 21, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the General Service Administration's (GSA) November 21, 2022 notice of a modified System of Records for Login.gov.[1] The GSA is revising the system of records to align with current National Institute of Standards and Technology technical standards and expanding the routine uses to include third-party fraud prevention. Login.gov is the secure sign-on service for the public to access various federal government websites and applications.

EPIC is a public interest research center in Washington, DC established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC regularly studies the

[1] 87 Fed. Reg. 70,819, https://www.federalregister.gov/documents/2022/11/21/2022-25420/privacy-act-of-1974-notice-of-a-modified-system-of-records

growth of and connections between government databases and advocates for strict controls on information flows to preserve privacy.[2]

EPIC commends the GSA for producing an accessible and thorough privacy impact assessment and supports further improving Login.gov to provide a single secure sign-on service across the federal government. EPIC urges the GSA to limit contracts for fraud prevention to a single third-party provider, to investigate and consider abandoning behavioral analytics techniques, and to carefully audit any risk-scoring practices by LexisNexis and provide a clear avenue for appeal when an account is flagged as potentially fraudulent.

I. Background

Login.gov is "a single, secure platform owned and operated by GSA through which members of the public can sign in and access information and services from participating federal agencies ('partner agencies')."[3] In September, 2022 the GSA updated its privacy impact assessment (PIA) for Login.gov in part to describe new fraud prevention tools the agency is implementing. The GSA contracted with LexisNexis to provide the following fraud prevention services for Login.gov:

- Confirm device integrity, characteristics, reputation and association with individual.
- Validate behavioral analytics, such as usage of mouse, keyboard, and interaction with the webpage.
- Confirm Internet Protocol (IP) address and email reputation.
- Protect against synthetic identities (false identities created by fraudulent actors).[4]

---

[2] *See e.g.*, Dana Khabbaz, EPIC, *DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information* (Aug. 2022), https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/; Comments of EPIC to the U.S. Postal Inspection Service on Using U.S.P.S. Customer Data for Law Enforcement (Jan. 18, 2022), https://epic.org/documents/epic-comments-to-the-u-s-postal-investigative-service-on-using-u-s-p-s-customer-data-for-law-enforcement/; Comments of EPIC on the U.S. Department of Homeland Security/ALL-046 Counterintelligence Program System of Records (Jan. 2021), https://epic.org/documents/u-s-department-of-homeland-security-all-046-counterintelligence-program-system-of-records/.

[3] Laura Gerhardt, GSA, *Login.gov Privacy Impact Assessment* at 5 (Sept. 19, 2022), https://www.gsa.gov/cdnstatic/logingov_PIA_September%202022.pdf (*hereinafter* Login.gov PIA).

[4] *Id*. at 8.

The PIA specifies that LexisNexis ThreatMetrix is the current provider of fraud prevention services, but the GSA contemplates contracting with multiple third-parties for fraud prevention.[5] In the past, the GSA has contracted with data broker TransUnion for fraud prevention services on Login.gov, though whether that contract remains in effect is unclear.[6] LexisNexis is also the primary third-party provider of identity-proofing services for Login.gov.[7] There is a separate privacy impact assessment for LexisNexis that covers both fraud prevention and identity proofing.[8]

II. The GSA should not obtain fraud prevention services from multiple service providers simultaneously.

In the Login.gov PIA and the proposed Login.gov SORN, the GSA leaves room to contract for fraud prevention services from multiple third-party providers. The GSA should restrict outside fraud prevention services to a single carefully vetted and audited third party to prevent increased risks of data loss and data breach. The Login.gov authentication process ingests a variety of personally identifiable information and provides that information to third party entities including:

- Full Name and Address
- Social Security Numbers
- Date of Birth
- Biometrics including Keyboard and Mouse behavior

[5] *See, e.g., id* at 23 ("Third-party providers only verify the information provided by the user and do not provide any information to partner agencies. third-party identity proofing services only send the following information back to login.gov: transaction ID; pass/fail indicator; date/time of transaction; and codes associated with the transaction data.").
[6] Alfred Ng, *Data brokers raise privacy concerns — but get millions from the federal government*, Politico (Dec. 21, 2022), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600; TransUnion, *TransUnion's NIST-Compliant Identification Managed Services Among First to be Awarded GSA's Approved Status Designation*, TransUnion Newsroom (Sept. 18, 2022), https://newsroom.transunion.com/transunions-nist-compliant-identification-managed-services-among-first-to-be-awarded-gsas-approved-status-designation/.
[7] Login.gov PIA at 18 n. 26.
[8] Laura Gerhardt et al., *LexisNexis Risk Solutions (LNRS)Identity Proofing Privacy Impact Assessment (PIA) – Guidance*, GSA (Sept. 15, 2022), *available at* https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems (*hereinafter* LexisNexis PIA).

- Device Information including Browser, IP address, and geolocation data[9]

This type of information is valuable and creates serious risks of identity theft, surveillance, and fraud if lost in a data breach or otherwise leaked from the third-party service provider.

Because of the sensitive nature of information that the GSA permits third parties to collect, the GSA should minimize the risk of data breach by limiting its fraud prevention services to a single provider. Multiple providers with access to the same data magnifies the risk of a data breach as that data is stored on multiple systems. The GSA is also more likely to be able to thoroughly vet a single provider than the multiple providers allowed for in the PIA and SORN.

III. The GSA should investigate and consider abandoning behavioral analysis fraud prevention.

Login.gov collects and discloses behavioral analytics including mouse and keyboard movements to LexisNexis for fraud prevention purposes.[10] This type of biometric collection records how a person moves their mouse, types on their keyboard, and otherwise uses their computer. Although behavioral analysis has some advantages for fraud prevention, neither the PIA nor the SORN contemplate potential drawbacks.

First, recording behavioral biometrics requires a third-party Javascript plugin to capture mouse movements and keystrokes on the Login.gov website. Although the Login.gov PIA discloses the use of behavioral analytics, it may not be clear to users of Login.gov that this type of monitoring is required to use the service. Further, providing notice alone means little when individuals have no practical alternative to using Login.gov to access federal government services. Therefore, the GSA should carefully scrutinize all forms of surveillance on Login.gov and seek to minimize the use of these surveillance technologies.

[9] *Id.* at 11-12.
[10] *Id.*

Second, this type of behavioral surveillance is an invasive form of monitoring. Tracking how individuals use computers risks revealing users' medical information. At least one study used mouse movements to identify mild cognitive impairments associated with Alzheimers' disease as an early diagnosis tool.[11] Behavioral monitoring is also likely to capture information about individuals with disabilities, including the blind, individuals with limited vision, and those with neuromuscular conditions. For example, mouse movements have been used to screen for Parkinsons' disease and similar conditions.[12] Internet users with disabilities may also be disproportionately flagged by poorly designed fraud monitoring tools because their behavioral patterns will differ from abled users. Behavioral analysis creates an additional risk of harm that must be accounted for.

IV. The GSA should carefully audit any risk-scoring practices by LexisNexis and provide a clear avenue for appeal when an account is flagged as potentially fraudulent.

Finally, risk scoring by algorithm is prone to errors and bias that must be accounted for. Neither the Login.gov PIA nor the SORN identify risk scoring as a practice that can have disparate impacts. And neither one explicitly requires an appeal process to protect individuals' access to federal government systems when an error in risk scoring occurs. For a thorough treatment of the harms associated with algorithmic scoring, see EPIC's Screening and Scoring Project[13] and our recent report, *Screened and Scored in D.C.*[14]

The GSA should subject any scoring algorithms, internal or external, to a third-party algorithmic impact assessment and provide an avenue of appeal when accounts are flagged as

[11] Adriana Seelye et al., *Computer mouse movement patterns: A potential marker of mild cognitive impairment*, Alzheimers Dement (Amst.) 472-80 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4748737/.
[12] Kryzstof Gajos et al., *Computer Mouse Use Captures Ataxia and Parkinsonism, Enabling Accurate Measurement and Detection*, Wiley InterScience (Jul. 8, 2019), https://movementdisorders.onlinelibrary.wiley.com/doi/10.1002/mds.27915.
[13] https://epic.org/issues/ai/screening-scoring/.
[14] Thomas McBrien et al., *Screened and Scored in the District of Columbia*, EPIC (Nov. 2022), https://epic.org/screened-scored-in-dc/.

fraudulent. If an account is flagged but individuals do not understand why they are denied access to government websites and given a means to appeal, the GSA risks preventing individuals access to vital government benefits and entrenching discriminatory patterns.

Conclusion

EPIC urges the GSA to carefully consider the use of fraud prevention services and institute additional best practices to reduce the risk of wrongful surveillance or data breach. EPIC supports the agency's efforts to improve Login.gov and specifically applauds the agency for a well-structured and accessible PIA that provides the public with meaningful information on how Login.gov works. For further questions, please contact EPIC Counsel Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

John Davisson
John Davisson
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Counsel