AMERICAN ASSOCIATION FOR JUSTICE®
The Association for Trial Lawyers

March 11, 2025

Committee on Rules of Practice and Procedure
One Columbus Circle, NE
Washington, DC 20544
RulesCommittee_Secretary@ao.uscourts.gov

RE: **Privacy Rulemaking and the Redaction of Social Security Numbers**

Dear Members of the Committee on Rules of Practice and Procedure:

The American Association for Justice (AAJ) is a national, voluntary bar association established in 1946 to strengthen civil justice, preserve the right to trial by jury, and protect access to the courts for those who have been wrongfully injured. AAJ previously submitted a comment with the National Crime Victims Bar Association (NCVBA)[1] to encourage the advisory committees to undertake rulemaking to consider the use of gender-neutral pseudonyms and pronouns as an important safety protection for minors escaping unfathomable abuse and violence. AAJ previously urged that claimants' Social Security Numbers (SSNs) be excluded as required identification during the rulemaking on Social Security Supplemental Rules, noting that the practice is prohibited by some local rules.[2] In response to the ongoing discussion on privacy involving the elimination of partial social-security numbers as identifiers, AAJ submits this additional comment to expand upon its concerns regarding the federal rules' privacy protections.

I. Privacy Concerns Are a "Real-World" Problem.

The January 2025 memorandum from the Reporters' Privacy Rules Working Group to the Standing Committee states, "there is no real-world problem that we need to solve right now."[3] AAJ strongly disagrees with this statement. In truth, the risk of data misuse is an omnipresent, pervasive, and evolving threat in every sector of American life, including the judicial system. According to the non-

[1] *See* rules suggestions 24-CV-F and 24-CR-C.

[2] Am. Ass'n for Justice, Comment Letter on Proposed Social Security Rulemaking (Sept. 18, 2019) (on file with author) ("AAJ strongly recommends against inclusion of a requirement that any part of a claimant's Social Security Number be part of the case file.").

[3] Reporters' Privacy Rules Working Group Memorandum, *in* Committee on Rules of Practice and Procedure Agenda Book 151 (Jan. 7, 2025), https://www.uscourts.gov/forms-rules/records-rules-committees/agenda-books/committee-rules-practice-and-procedure-january-2025.

partisan Pew Research Center, the American public does not believe that it has too much privacy.[4]

That comprehensive survey also found:

- About a quarter of Americans (26%) have dealt with a fraudulent credit or debit card charge over the past 12 months.
- Eleven percent say that someone has hacked their email or social media account.
- Seven percent report that someone has attempted to apply for a loan or line of credit using their name.[5]

In total, 34% of Americans have experienced one of these issues over the last 12 months, and yet, the continued use of the last four digits of one's SSN seems to be acceptable practice. While a proposed amendment eliminating the use of the last four digits of SSNs would not eliminate the risk of identity theft, it could certainly lessen the risk of exposure to preventable harm to litigants.

II. The Use of Social Security Numbers Puts Americans at Risk for Identity Theft.

The data on the vulnerabilities regarding the use of social security numbers is long-established and extensive. The seminal study on social security numbers was published in 2009 by Carnegie Mellon professors Alessandro Acquisti and Ralph Gross, who found that social security numbers have the same safety level as a three-digit pin.[6] This research determined that with the right methods, SSNs can be predicted 0.9% of the time.[7] In some smaller states, *prediction rates exceeded 10%*.[8] Social Security numbers are also viewed as the most valuable piece of information in identity theft:

> SSNs remain easy to obtain. They appear in public documents such as court filings, tax lien records, property records, death certificates, and even missing persons reports. Additionally, the widespread leakage of SSNs by the private sector has increased the ease with which one can learn a potential victim's SSN.[9]

Importantly, SSNs were never designed to be used for security or identity purposes.[10] Their original purpose—to facilitate Social Security retirement payments—began long before the creation of the

---

[4] The Pew Research Center found that seven in ten adults (71%) say they are concerned about in 2023, up from 64% in 2019. Michelle Faverio, *Key Findings About Americans and Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

[5] *Id*.

[6] Alessandro Aquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106(27) PROC. NAT'L ACAD. SCIS. 10975 (July 7, 2009), http://doi.org/10.1073/pnas.0904891106.

[7] *Id*. at 10978.

[8] *Id*.

[9] Kathryn Witchger et al., *Semi-Secure Numbers? Augmenting SSNs in the Authentication Use Case*, 2019 J. L. TECH. & POL'Y 79, 88, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121116.

[10] Shoshana Weissman, *The Government Doesn't Care If a Child's Social Security Number Is Used for Fraud—Even Before They're Born*, R ST. (Aug. 26, 2024), https://www.rstreet.org/commentary/the-government-doesnt-care-if-a-childs-social-security-number-is-used-for-fraud-even-before-theyre-born/ ("Until recent history, SSNs were sometimes used as regularly as names . . . the purpose of the number was to keep track of Social Security retirement payments.").

internet, online payment systems, and widespread and routine identify theft.

Additionally, the SSN may contain identifying geographic markers that were removed in 2011 in favor of randomization.[11] Thus, if you were born before 2011, your SSN resembles that of any siblings born in the same household. A lot of valuable information can be obtained by a bad actor from a court record that provides a name, the last four digits of the SSN, and the year of birth. A study by ID Analytics in 2010 found that 5 million SSNs attached to three or more people.[12] Even a SSN randomly generated by a bad actor has a 50/50 chance of belonging to a person.[13]

In another study, researchers explored the "synthetic identity attack," which is when an attacker will use a valid SSN, often belonging to a child victim, coupled with another victim's name and identifying information to open fraudulent accounts.[14] This is often easier to accomplish with children, whose credit may not be regularly monitored, and provides an additional reason for protecting the SSNs of minors in court documents.

The SSN is also a valuable asset that can be sold on the black market.[15] Scammers can impersonate clerk employees and demand money to avoid being served with a summons.[16] While it may be more difficult to spoof the federal clerk's office, it is not impossible.[17]

---

[11] As the AARP has detailed, "The first three digits represented where a person was living when their SSN was issued (the numbers varied by state and got higher moving east to west). The next two represented blocks of numbers within that geographic area. The last four were a "serial number" to identify each individual within that block." *Are Social Security Numbers Reused?*, AARP (July 15, 2025), https://www.aarp.org/social-security/faq/do-identification-numbers-get-reused/

[12] ID Analytics is a company that helps businesses determine whether a customer is an actual customer or a bad actor. For businesses, the company is looking for the same person connected to multiple SSNs. For this research, the company reversed its work, examining SSNs that are connected to multiple people. *See* Bob Sullivan, *Odds Someone Else Has Your SSN? One in 7*, NBC NEWS (Dec. 3, 2010), https://www.nbcnews.com/technolog/odds-someone-else-has-your-ssn-one-7-6c10406347.

[13] *See* Weissman, *supra* note 10 ("[B]ad actors commonly use SSNs with a name that does not correspond to it. Moreover, because the SSA does not check SSNs before assigning them to newborns, it could easily assign a number that already has a history of arrests and financial problems.")

[14] Witchgar et al., *supra* note 9, at 87.

[15] Any individual SSN can retail for as little as $4 on the darknet, according to two-year study on the cost of fake passports, compromised bank accounts and other information available for sale on the dark web. Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web*, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/

[16] Scammers impersonated the court clerk in Palm Beach County with the number appearing to come from the clerk's office. This scam is known as spoofing. Press Release, Joseph Abruzzo, Clerk of the Circuit Court & Comptroller, Palm Beach Cnty., Fla., Fraud Alert: Scammers Impersonating Clerk Employees in Fake Calls, https://www.mypalmbeachclerk.com/about-us/news/fraud-alerts/scammers-impersonating-clerk-employees-in-fake-calls (last visited Mar. 3, 2025).

[17] Multiple district courts post warnings regarding fraud and scams. One common type of scam is a call from a person purporting to be from the U.S. Marshall's office demanding a fee or a late payment fee for someone who allegedly skipped jury service or failed to pay a fine. *See Fraud Alerts*, D. Md., https://www.mdd.uscourts.gov/fraud-alerts (last visited Mar. 5, 2025); Press Release, U.S. Atty's Off., M.D. Fla., U.S. District Court and U.S. Attorney's Office Warn Public of Jury Duty Scam (Jan. 8, 2024), https://www.justice.gov/usao-mdfl/pr/us-

III. Privacy Is Collective Responsibility.

It is incumbent upon all of us—individuals, employers, the government, and the court—to protect privacy. Hackers, bad actors, and cyber threats are everywhere. The absence of an obvious case or archetypal rules issue does not absolve the rules committees from their role in the collective responsibility to modernize the judiciary's privacy practices. This obligation to take proactive measures is especially critical since it would be extremely difficult to bring an individual claim showing that one's identity was stolen, hacked, or otherwise compromised by the required disclosures in a court filing. In the first place, if one is already a named party in a case, the resolution of the case is likely a higher priority. Secondly, privacy claims associated with fraud and identity theft will require a class action to address the cause of harm.[18] Failure to address an issue until there is evidence of a problem does not align with the values of fairness and justice.

IV. AAJ Urges Full Redaction of SSNs.

Americans must worry about their private information being hacked from their personal phones and computers, the businesses where they bank and shop, their employers, and even the government. The courts should help parties by not contributing to the risk of identity theft and other privacy violations. The advisory committees should take steps to reduce the risk of harm by removing SSNs from court filings. AAJ supports the effort of the Advisory Committee on Criminal Rules to address privacy issues[19] and urges the Joint Committee on Privacy to reconsider its recommendations.

Conclusion

AAJ supports amending Fed. R. Civ. P. 5.2(a) and Fed. R. Crim. P. 49.1(a) to require the full redaction of SSNs in public filings, as well as the use of gender-neutral pseudonyms and pronouns, rather than initials, in reference to minors and their guardians. AAJ encourages the civil and criminal advisory committees to move forward with these proposals. If we can be of further assistance or provide additional information on privacy safety practices, please contact Sue Steinman, Senior Director of Policy and Senior Counsel, at susan.steinman@justice.org.

Respectfully Submitted,

Lori Andrus
President
American Association for Justice

---

district-court-and-us-attorneys-office-warn-public-jury-duty-scam; and *Jury Scam Alerts*, D.D.C. https://www.dcd.uscourts.gov/jury-scam-alerts (last visited Mar. 5, 2025).

[18] Unfortunately, a class action would be hard to bring if identity is stolen through individual court filings. Stolen data would also likely be sold to aggregators making the perpetrator difficult to trace as well as there may not be enough class members to establish the claim as a class.

[19] *See, e.g.*, Rule 49.1 Subcommittee Report, *in* Advisory Committee on Criminal Rules Agenda Book 239–40 (Nov. 2025), https://www.uscourts.gov/sites/default/files/2024-12/2024-11-criminal-rules-meeting-agenda-book-final-revised-12-6_0.pdf ("[M]embers were unable to identify any reason that the last four digits were needed in public filings.")