Regarding SF 2885:

- There are three major sections which are bizarre and disastrous public policy. Section 2 and 4 and 5.
- Section 2, does two things, makes email addresses and phone numbers in almost every public document secret (private). Page 2, lines 4 and 5.
- Then on lines page 2, lines 15 through 22 allows the government to use that contact info for almost any purpose.. No other state has done this.
- No state applies a blanket secrecy rule for every email address and phone number across nearly all public documents.

There are consequences for public accountability if done. I share that below:

1) Reduced transparency and accountability
   Keeping citizen contact information public enhances transparency, allowing the public to see who is interacting with the government. In dynamics and settings in government where many times emails are sent, and the only identifying data is their email address ,knowing who communicated with a Director of agency on a public concern, for example, can help verify its authenticity and foster trust. .
2) Hindered Communication and Collaboration
   The proposal would limit communication, affecting collaboration. For example, in community and neighborhood projects, individuals might want to connect with others who have interacted with the government , such as in zoning applications, to work together on local issues.
3) Impact on research and reporting
   Journalists and researchers often rely on public documents to contact individuals for follow-ups or verification, and making contact info such as email address secret would impede this.
4) Administrative complexity
   Managing a system where individual contact information is kept secret in public documents could add complexity to government operations.
5) Balancing privacy and public interest
   While privacy is important, a blanket policy of secrecy which is being proposed here is not the best way to balance it with the public's right to know. For instance, some citizens might want their phone number or email address public for networking, and a one size fits all overlooks this.
6) Current law allows for redactions under certain conditions, but a basically a blanket policy of secrecy for all citizen contact info would be a significant shift in public policy
7) Then allowing the government to use the contact info for almost any purpose is totally absurd. My arguments against that are as follows:
8) Privacy concerns
   The most immediate issue is the erosion of personal policy. If the government has unrestricted access to your contact information, it can be used for purposes beyond what you intended when providing it, such as sending unsolicited messages

or even engaging in intrusive monitoring. This lack of boundaries which the proposal has risks making individuals feel their personal space is violated.

9) Data security risks
   Storing large amounts of contact information creates a target for hackers. If the government's systems are breached, your email and phone number could be exposed, leading to identity theft, or other cyber crimes. The more purposes the data is used for, the more systems it may be stored on, increasing this vulnerability.
10) Lack of consent
   You might provide your email or phone number for a specific reason, like registering for a service, but not expect to be used by the government for unrelated purposes. Without clear, informed consent for each use, this proposed policy violates your right to control how your personal information is handled.
11) Lack of transparency
   Without clear rules about how your information is being used, you're left in the dark. If the government isn't open about its purposes, whether it's for public health outreach or something more controversial, you cannot hold it accountable or challenge misuse. You are also not given a Tennessen warning.
12) Mission creep
   What starts as a limited use of your contact info could expand over time. For instance, data collected for one purpose might later be used for unrelated initiatives, all without additional approval or oversight.
13) Data retention issues
   If the government can use your email and phone number for any purpose, it might keep them indefinitely.. Without strict policies on how long data is stored or when it's deleted, your information could linger in systems, amplifying the risk of misuse or leaks over time.
14) Chilling effects
   Knowing the government could use your contact details for anything might make you hesitant to share that data at all. This could reduce your willingness to engage with public services, i.e.
15) Erosion of trust
   If the government misuses or abuses this power, say by spamming you, for example, it damages trust. When people feel their information is not safe or respected, confidence in government.
16) Sections 4 and 5 dealing with records management and official records.
   I believe this should not go forward without broad discussion with an array of interested parties from historians, archivists, open government people to researchers. Hennepin County in their rationale statement for this proposal states there is a federal directive for digitization. Hinting that the states must do it. It is not a legal requirement for states to do so.
17) There are issues with these sections that need to be discussed more thoroughly in the following areas:
   Loss of original records
   Long term preservation challenges

Authentication and integrity issues
Format variability and standardization
Public access
Cost and resource implications
Legal and evidentiary concerns

18) What does the state archivist think of Hennepin County's proposal?

So that's it. I share this with you to help you inform your members.

Any questions, call or contact me.

Rich Neumeister