The Administrative Conference has issued several recommendations to help agencies balance the competing considerations of transparency and confidentiality in managing their rulemaking dockets. This project builds on these recommendations. It provides greater specificity to agencies on how they should handle rulemaking materials they determine should be withheld to protect sensitive business or personal information, notwithstanding any countervailing benefits of disclosure (hereinafter “protected material”).

As part of the rulemaking process, an agency creates a public rulemaking docket, which consists of all rulemaking materials the agency has: (1) proactively published online or (2) made available for public inspection in a reading room. Public rulemaking dockets include materials agencies generate themselves and comments agencies receive from the public. Broadly speaking, public rulemaking dockets serve three purposes: providing the public with the information the agency considered in a rulemaking, providing courts with a record for evaluating challenges to the rule, and satisfying agency recordkeeping requirements.

Currently, agencies accept public comments for their public rulemaking dockets through Regulations.gov and their own websites. Regulations.gov and agency websites that accept comments expressly notify the public that the agency may publish the information it receives.¹ When a person submits a comment to an agency, however, the agency does not immediately publish the comment. Instead, agencies take time to review comments before publishing them. Most agencies perform at least some kind of screening during this period.

Agencies perform this screening because, in maintaining their public rulemaking dockets, they confront competing considerations of transparency and confidentiality. On the transparency side, the Freedom of Information Act (FOIA) presumes disclosure of information requested by a member of the public, subject to certain exceptions described below. And the Portland Cement doctrine requires agencies to make publicly available the critical information — including technical studies, staff reports, data, and methodologies — underlying proposed rules.³

But agencies often receive materials during rulemaking for which the law authorizes withholding because of their content. For example, one of FOIA’s exemptions, called “Exemption 6,” covers “personnel and medical files and other similar files the disclosure of which would constitute an unwarranted invasion of privacy.”⁴ “Similar files” means any information about a person, such as a name, address, or occupation, that can be used to identify the person.⁵ In deciding whether Exemption 6 applies, courts determine whether disclosure would constitute a “clearly unwarranted invasion of personal privacy.”⁶ In making this determination, they balance the privacy interests of the person to whom the information pertains against society’s interest in learning about governmental processes. Privacy interests are greatest

---

⁵ See Sherman v. U.S. Dep’t of Army, 244 F.3d 357, 361 (5th Cir. 2001).
when the projected harm from disclosure of the information includes identity theft and fraud.\(^7\) Privacy interests are minimal when a person has consented to the agency disclosing his or her information. If an agency encounters information that falls under Exemption 6, FOIA authorizes the agency to exclude it from the public rulemaking docket.

Another FOIA exemption, called “Exemption 4,” covers “trade secrets and commercial or financial information obtained from an individual and confidential.”\(^8\) Information is “confidential” within the meaning of Exemption 4 if it is “customarily . . . kept private or closely held by the submitter” and the government has given some assurance to the submitter, either explicitly or implicitly, that the information will not be publicly disclosed.\(^9\) The Recommendation refers to these materials collectively as “confidential commercial information.” An agency can assure a submitter that confidential commercial information will not be publicly disclosed by, for example, directly communicating to the submitter an intent to not disclose his or her confidential commercial information, posting a general notice informing submitters that their confidential commercial information will not be disclosed, or engaging in an established practice of not disclosing confidential commercial information.\(^10\) FOIA authorizes agencies to exclude from their public rulemaking dockets information falling under Exemption 4.

There are three categories of material that agencies generally consider to be “protected materials.”\(^11\) The first is unique identification numbers, either of submitters themselves or of third parties, that create a high risk of identity theft if disclosed. This category includes social security numbers, bank account numbers, and passport numbers. The second category consists of two kinds of information: information about the submitter submitted to the agency accidentally,
and information pertaining to someone other than the submitter. Information within this category includes names, email addresses, physical addresses, medical information, and so on. The final category consists of confidential commercial information provided to the agency under an assurance of protection from disclosure. Courts have generally authorized agencies to withhold materials in all three of these categories under FOIA Exemptions 4 and 6.¹²

This Recommendation prescribes steps agencies can take to exclude from their public rulemaking dockets protected material while still providing the public with the information upon which the agency relied in formulating the proposed rule. These steps include, among others, aggregating the data, which means delinking the data from the individuals to whom the data belong and then presenting the data in a summarized form, such as a median. The Recommendation also identifies resources that can help agencies implement the principle of excluding from their public rulemaking dockets protected material while still providing the public with the information upon which the agency relied in formulating the proposed rule.

**RECOMMENDATION**

**Including Notifications for Members of the Public Before They Submit Comments or Otherwise Take Part in Rulemaking**

1. Agencies should decide which classes of rulemaking materials should be withheld to protect sensitive business or personal information, notwithstanding any countervailing public benefits of disclosure (hereinafter “protected material”). In making this decision, agencies should be aware that other agencies generally deem the following classes of material to be protected material:

   a. Unique identification numbers including social security numbers, bank account numbers, and passport numbers;

   b. Medical information

   c. Financial information

   d. Personal information

   e. Business information

1² See, e.g., Taitz v. Astrue, 806 F. Supp. 2d 214, 220 (D.D.C. 2011) (authorizing, under Exemption 6, withholding of social security numbers); Schoenman v. FBI, 573 F. Supp. 2d 119, 149 (D.D.C. 2008) (authorizing, under Exemption 6, withholding of information pertaining to third parties); Food Marketing Inst., 139 S. Ct. at 2361 (authorizing, under Exemption 4, withholding of confidential commercial information provided to the agency under an assurance of protection from disclosure).
b. Names, email addresses, physical addresses, incomes, medical information, and other kinds of personal information inadvertently submitted by the commenter or that pertain to third parties; and
c. Confidential commercial information provided to an agency under the agency’s assurances of protection from disclosure.

2. To reduce the risk that agencies will inadvertently disclose protected material in connection with rulemakings, agencies should clearly notify the public about their treatment of protected material. An agency’s notifications should:

   a. Inform members of the public that all comments submitted are subject to public disclosure;
   b. Instruct members of the public how they can submit comments anonymously, for example, by writing “Anonymous” in the name field on the online comment platform or by leaving the name field blank;
   c. Inform members of the public what weight, if any, the agency accords comments that are submitted anonymously;
   d. Inform members of the public whether the agency offers assurances of protection from disclosure for their confidential commercial information and if so, how to identify such information for the agency;
   e. Instruct members of the public never to submit unique identification numbers such as social security numbers and other kinds of personal or confidential commercial information that pertain to third parties, such as medical information and trade secrets;
   f. Advise members of the public to review their comments for the material identified above in e. and, if they find such material, to remove it;
   g. Inform members of the public that they may request, during the period between when a comment is received and when it is made public, that personal information they inadvertently submitted be withheld;
   h. Inform members of the public that they may request, after the agency has published any comment, that personal or confidential commercial information

Commented [TR3]: ACUS staff proposes moving this language to the Preamble and combining/reconciling it with language at 51-60.

Commented [TR4]: Adam J. White suggested a recommendation that encourages agencies, or perhaps the General Services Administration (GSA), to create a box that a member of the public could check to indicate that he or she is submitting confidential commercial information or personal information.

Commented [TR5]: The Committee began discussion of b. and c. last meeting, but did not reach a resolution. We informed the Committee that another ACUS project, titled Mass, Computer-Generated, and Fraudulent Comments is addressing the topic of anonymous comments and that we would provide the Committee with a description of that project as it relates to this topic. That description appears below:

One of the key issues addressed in the Mass, Computer-Generated, and Fraudulent Comments project will be whether or not the identity of the commenter matters, as it bears on whether or not agencies are likely to see mass, computer-generated, or fraudulent comments as a problem. The research team will therefore be interviewing agencies about whether or not they allow anonymous comments and, if so, whether and how those comments are treated differently from other comments. The project report and recommendation may ultimately contain one or more recommendations relating to anonymous comments insofar as they are relevant to agencies’ efforts to address mass, computer-generated, and fraudulent comments.
pertaining to themselves or to their dependents within the comment be
removed from public exposure; and
i. Inform members of the public that the agency reserves the right to redact or
aggregate any part of a comment if the agency determines that it constitutes
protected material, or may withhold a comment in its entirety if it determines
that redaction or aggregation would insufficiently prevent the disclosure of
this information.

3. An agency should include the notifications described in Paragraph 2 in at least the
following places:
   a. Within the rulemaking document upon which the agency requests comments, such
      as a notice of proposed rulemaking or an advanced notice of proposed
      rulemaking;
   b. Within the online comment submission form on Regulations.gov, or, if the agency
does not participate in Regulations.gov, on the agency’s own comment
      submission form;
   c. Within any automatic emails that an agency sends acknowledging receipt of a
      comment;
   d. On any part of the agency’s website that describes its rulemaking process; and
   e. Within any notices of public meetings pertaining to the rule.

Deciding Whether To Offer Assurances of Protection from Disclosure For
Confidential Commercial Information

4. Agencies should recognize that there may be instances in which businesses want to
submit confidential commercial information, such as trade secrets, to inform the
agencies’ rulemaking efforts, but do not want such information to be made publicly
available. Agencies should decide whether they will offer assurances of protection from
disclosure for confidential commercial information. Factors that weigh in favor of

offering assurances of protection from disclosure include:

a. The agency has the resources to identify and withhold confidential commercial information;

b. The agency receives a high volume of requests for protected treatment of confidential commercial information;

c. The agency’s rulemaking efforts can benefit from the agency’s review of confidential commercial information; and

d. The agency can identify no substitute for confidential commercial information that would inform its rulemaking in a comparable manner.

5. Agencies that choose to offer assurances of protection from disclosure for confidential commercial information should decide how they will offer them. Agencies can choose to inform submitters, directly upon submission, that they will accord confidential commercial information protected treatment; post a general notice informing submitters that confidential commercial information will be accorded protected treatment; or both.

6. Agencies that choose to offer assurances of protection from disclosure for confidential commercial information should adopt policies to help them identify such information. Agencies should consider including the following, either in tandem or as alternatives, as part of their policies:

a. Instructing submitters to write the word “Private,” “Protected,” or similar language within the header of their submissions that contain confidential commercial information;

b. Instructing submitters to flag the particular text within the comment that constitutes confidential commercial information; and

c. Instructing submitters to submit both redacted and unredacted versions of a comment that contains confidential commercial information.

7. Agencies that choose to accord protected treatment for confidential commercial information should withhold such material, using the techniques described in Paragraph 11 as appropriate.
Allowing Submitters to Notify the Agency of Material They Inadvertently Submitted

8. Agencies should give submitters an opportunity to alert relevant agency officials to any personal information they inadvertently included in their comments.

9. Agencies should ensure that the personal information submitters have identified as inadvertently submitted is not publicly disclosed, or, if already disclosed, is removed as promptly as possible.

Allowing People to Notify the Agency, After the Agency Publishes the Comment, of Personal and Confidential Commercial Information They Want Removed

10. Agencies should allow people to request that personal or confidential commercial information pertaining to themselves or a dependent within the comment be removed from public exposure. Agencies should review such requests and, upon determining that the information subject to the request is, in fact, personal or confidential commercial information, they should take all steps necessary to so remove it.

Screening Comments for Protected Material and Protecting Such Material from Disclosure

11. Agencies should screen comments for protected material. If, when screening, an agency determines that a comment contains:

   a. *Isolated instances of protected material*, the agency should redact that material and publish the rest of the comment. Redaction should be thorough enough to prevent a person from discerning the redacted information, but not so broad as to prevent the public from viewing non-protected material;

   b. *Protected material pertaining to a large number of people*, the agency should delink the data from the individuals to whom the data belong and present the data in a summarized form, such as an average (hereinafter “aggregation”). Agencies should work with data science experts and others in relevant disciplines to ensure
that aggregation is thorough enough to prevent someone from disaggregating the
data (i.e., linking the aggregated data with any person).

12. If redaction and aggregation would still permit a member of the public to identify the
redacted material, or disaggregate the aggregated material, the agency should withhold
the comment in its entirety.

13. Agencies should explore using a variety of computer-based tools to aid in their
identification of protected material. This exploration should include speaking with private
sector experts and technology-focused agencies such as the General Services
Administration’s Technology Transformation Service and the Office of Management and
Budget’s United States Digital Service to determine which tools are most appropriate and
how they can be best deployed given the agencies’ resources.

Describing Material an Agency Has Withheld

14. When agencies withhold from public disclosure personal or confidential commercial
information they have received from the public in connection with a rulemaking and on
which they have relied in formulating rules, they should describe the withheld material in
as much detail as possible without compromising its confidentiality. In doing so, agencies
should consider preparing explanatory staff or technical reports and should publish these
reports on the parts of their websites that describe their rulemaking processes and within
the preambles to final rules.