Stay Safe in the Public Eye

Resources for Scientists and Experts

As a scientist, your voice is needed in the public sphere. But speaking up can be risky sometimes. Some scientists are facing digital threats, harassment, and reputational attacks for their public engagement—or even just doing their jobs. The guidance and resources outlined below can help you safely engage.

Know Your Risks and Assess Your Exposure

As the coauthors of *The Anti-Autocracy Handbook: A Scholars' Guide to Navigating Democratic Backsliding* write, "In a democracy, citizens should not suffer any consequences for peaceful opposition to the government. If people or institutions are incurring a cost for opposition, then this should enter into the risk assessment." Unfortunately, there have been costs for scientists and advocates in speaking out against attacks on science and our democracy; therefore, knowing your risks and taking action strategically are critical.

The Anti-Autocracy Handbook also notes that "Risk assessment is subjective, uncertain, and may require revision." That's because risk assessment is context-dependent: it's not only dependent on the facts of a situation, but also on how we *perceive* the context, what information we have about the context and risk levels, and how our personal factors may vary over time. Risk assessment is an ongoing conversation you should have with yourself and those in your circles.

The risk assessment table on p. 2, adapted from a table created by Dr. Christina Pagel, can help you assess both your personal and reputational risk levels based on your personal demographics, history, political visibility, current context, and institutional factors.

Assessing Your Risk Exposure

There are some actions that everyone can take regardless of your level of risk, including: building community, taking care of your mental health, committing to upholding facts and evidence in the face of rampant disinformation, and taking steps to enhance your digital security and understanding of digital risks. Beyond these, different types of engagement like submitting a regulatory comment, speaking at a rally, serving as an expert witness, or talking to the media carry different levels of risk. In addition to assessing the range of risks outlined in the table, ask yourself the following questions before engaging:

- **Public records:** How exposed are my work and communications? Could my emails, notes, or other documents (whether published or draft) be subject to federal Freedom of Information Act (FOIA) or state open-records requests? Do I communicate with anyone who could be subject to open-records requests, either directly or via a listserv? Similarly, who else might be targeted or harassed based on disclosures of my communications?
- **Institutional role:** When I participate in public discussions, am I being clear about whether I am speaking in a personal capacity or on behalf of my institution? Could my statements and/or participation be misinterpreted as representing my institution without authorization?
- **Personal exposure:** What personal details (e.g., address, phone, email, family members, photos) can be found with an online search?
- **Digital hygiene:** Do I practice good habits online? Have I considered how past posts, comments, or online activity might be taken out of context or misused? What settings or retention policies can I update to minimize my risk exposure?
- **Institutional support:** If I am targeted, does my institution have resources (legal counsel, ombuds office, insurance, communications staff) and the political will to support me? Could my interests conflict with the interests of the institution? What other support might I need?
- **Credibility:** Do I have clear documentation and citations to back up my key claims if challenged? Could any of my past publications, statements, or affiliations be taken out of context to challenge my expertise?
- **Harassment preparedness:** What is my plan for handling hostile emails, online attacks, or misrepresentation in the press? Have I identified trusted colleagues, allies, and resources I can turn to quickly if harassment escalates?

Personal and Reputational Risk Assessment Factors

Demographics		Personal History		Personal Political Visibility		Personal Current Context		Institutional Factors	
Factor	**Score**	**Factor**	**Score**	**Factor**	**Score**	**Factor**	**Score**	**Factor**	**Score**
Targeted ethnic group	3	Police record (however trivial)	2	Public profile as regime critic	2	Main household earner	2	Institution unlikely to support you if targeted by regime	1
Targeted religious group	3	Tax issues	2	Media (newspaper, broadcast, podcast) activity with negative comments on regime	2	Primary caretaker	2	Ambiguous policies around institutional support	1
Not a national citizen	3	Immigration violations at any point	2	Social media activity with negative comments on regime	1	Financial difficulties	2	Lack of policies around institutional support	1
Temporary visa status	2	Any other brush with officials at any point	1	Journal publications on topics that are out of favor with regime	1	Insecure employment	2		
Gender nonconforming	2			Prominent attendance at regime-critical political events or protests	1	Poor health	2		
LGBT+	1					Household members who are vulnerable	1		
Female	1								

Cumulative Score	Risk Category
0–4	Low
5–9	Medium
10–14	High
15+	Extreme

This table is designed to help you assess the level of risk you may face, personally and/or professionally, by engaging in the public sphere. These decision points should be considered by you as an individual, and not used to make assumption about others.

SOURCE: ADAPTED FROM *THE ANTI-AUTOCRACY HANDBOOK.*

Protect Your Digital Footprint

Digital security is foundational. Good practices not only reduce the risk of hacking or harassment, but also help prevent sensitive research materials or personal communications from being taken out of context.

- If you work for a government agency or public university, always assume that your emails, notes, and data can be made public.
- Know your institution's records-retention policies and follow them. These may dictate how long emails or documents are kept, either by the institution or by individuals, and when they must be archived or deleted. If your institution doesn't have a records-retention policy, advocate for one to be implemented.
- Use strong passwords and two-factor authentication. Encrypt devices and keep software updated to reduce security vulnerabilities.
- Limit the personal information that appears online. Consider removing home addresses, personal phone numbers, and family details from websites, directories, and/or social media posts. Use a data removal service to monitor and remove your personal information online for an annual or monthly fee.
- Periodically review your online presence (i.e., Google yourself) as if you were an adversary searching for weaknesses.

Additional Resources:

- **Safeguarding Online Communications**
  Detailed best practices for email, devices, and social media
- **Personal Security Assessment**
  Step-by-step guide to evaluating digital safety risks
- **Digital Security Zine**
  Accessible, creative guide to digital safety for activists and experts

Understand Public Records Laws, Institutional Policies, and Available Resources

If you're a scientist with a government agency or public university, you should assume your emails, notes, and data may become public under federal FOIA or state-level open-records laws. If you're employed at a private institution, correspondence with those at public institutions may be subject to similar laws. Protections vary widely across states: some exclude or exempt research records, while others provide little protection. Here are some practical steps:

- Familiarize yourself with your state's specific laws. CSLDF maintains a state-by-state guide of open-records laws and research protections.
- Always write emails using careful and professional language, with the assumption they could be disclosed. In contrast, conversations that create no records—such as in-person discussions, phone calls, or Zoom meetings (without transcript or recording)—will be the most likely to stay private.
- Build relationships with institutional staff like legal counsel, ombuds offices, union representatives, or compliance staff. These existing relationships will be critical when asking for support in handling requests.
- Always seek advice before complying with a request for records. Advice can come from institutional staff, or from trusted third parties.
- When engaging in a public forum as a public citizen, maintain a clear distinction between your personal and professional roles, including by using disclaimers such as "affiliation for identification purposes only."

Additional Resources

- **Security Threats Model**
  Framework for assessing risks to researchers
- **Researcher Support Resources**
  Practical tools for protecting researchers at risk

Plan for Potential Harassment and Intimidation

Harassment and intimidation can disrupt both your personal and professional life. Preparing and maintaining a clear response plan can not only reduce their impact but also increase your overall resilience. Many of these strategies enhance general professional safety, but are particularly critical when facing targeted harassment.

- **Limit exposure.** Remove your personal details from online directories and review what is visible on social media. If necessary, contact other account holders or the platform itself to ask for your information to be taken down.
- **Set a response protocol.** Identify whom to contact within your institution (e.g., department chair, ombudsperson, human resources department, security office) if harassment occurs so they may respond appropriately. Identify others in your network (research collaborators, funders, etc.) who should be notified.
- **Keep records.** Save harassing emails, messages, or voicemails; take screenshots where useful from social media or other online platforms. Documentation is critical if escalation occurs.
- **Anticipate media pressure.** Controversial topics sometimes attract hostile press attention. Media training can help you communicate clearly and avoid being misquoted. Set up a Google Alert to track if you are named in any blogs or media.
- **Build external support.** Professional societies, advocacy groups, and legal aid organizations can provide assistance and support if harassment intensifies.

Additional Resources:

- **Handling Political Harassment and Intimidation**
  Best practices for responding safely
- **Science in an Age of Scrutiny**
  Guide on responding to criticism and personal attacks
- **Know Your Risks (National Lawyers Guild)**
  Tips on recognizing risks and protecting yourself while speaking out
- **Climate Whistleblowers**
  Support network for individuals exposing climate-related misconduct
- **Speaking Up for Science: A Guide to Whistleblowing for Federal Employees**
  Guide to help federal employees identify and speak out about abuses by political leadership

Engage Professionally in Public Processes

Participation in policymaking is a powerful way to apply your expertise. Robust science, clear boundaries, solid preparation, and reliable support ensure protection for you and your circle of colleagues, collaborators, supporters, and loved ones.

- **Provide evidence-based input.** Always cite peer-reviewed studies, link to published data, and explain methods clearly. Avoid ascribing intent or motivation.
- **Disclose potential conflicts of interest.** Transparency builds credibility.
- **Expect public scrutiny.** Your qualifications, past publications, statements, and affiliations will come under the microscope; review them for consistency in advance.
- **Keep a record of what you submit or testify to.** Comments and testimony often become part of the public record, but maintaining a record of your own public engagement may be helpful as a backup.

As noted in a 2025 *Science* editorial, "We know from other countries and contexts that aspiring authoritarians often target scientists, elevate loyalists, and suppress or sideline any who might have the knowledge, expertise, or power to challenge government transgression and failures to make science-based policy decisions." As trusted and credible messengers in our society, scientists must use the trust the public has placed in us to continue advancing research for the public good, speaking out, and taking action in support of science and democracy.

Additional Resources and Readings

- **Science Advocacy Training Series**
  UCS resources on effective advocacy and communication for scientists
- **Resources for Federal Scientists**
  Guidance and other broadly relevant tools for scientists working within or alongside federal agencies
- **Independent Science Initiative**
  Overview of the many independent science efforts currently under way, including in-depth resources for establishing or supporting an independent science advisory committee
- ***The Anti-Autocracy Handbook***
  Guidance to scholars navigating the growing global trend of democratic backsliding and authoritarianism, plus a framework for action based on personal risk level
- **Know Your Rights: Scientific Activism and Protests**
  A guide for scientists on how to safely exercise their rights to engage in protest and advocacy

Union of Concerned Scientists

www.ucsusa.org/resources/scientist-advocacy-toolkit

The Union of Concerned Scientists puts rigorous, independent science into action, developing solutions and advocating for a healthy, safe, and just future.

HEADQUARTERS
Two Brattle Square
Cambridge, MA 02138
617-547-5552

WASHINGTON, DC
1825 K St. NW, Suite 800
Washington, DC 20006
202-223-6133

WEST COAST
2001 Addison Street, Suite 200
Berkeley, CA 94704
510-843-1872

MIDWEST
200 E. Randolph St., Suite 5151
Chicago, IL 60601
312-578-1750

ONLINE