When to Go Public When Attacked? Some Considerations

October 2017

Security and shared knowledge are power.
Security is a process, not an event.
Security is Solidarity.

Politically motivated opposition attacks are on the rise. They include attacks on grantees of foundations and, increasingly, attacks on foundations that fund organizations engaged in high profile social change work. These range from PR smears, to harassment of individuals, to data breaches and revelation of strategic plans and confidential landscape assessments.

During the two "Weathering the Storms (WTS) for Foundations" workshops in May-June 2017, there was considerable conversation regarding if and when foundations should be public about attacks they have experienced or may experience in the future. RoadMap was asked to offer some written guidance regarding this question. Based on our experience of supporting social justice organizations and alliances that are under attack or who are likely targets of attacks we offer the following guidance for your consideration.

Attacks by opposition forces naturally bring on a range of emotions and reactions. These range from fear and embarrassment, to confusion, anger or denial. It's important to be aware of all of these emotions in the aftermath of an attack, and to create organizational space to acknowledge and validate any and all emotions that may come up.

Why You Should Go Public: **Four good reasons**

- **Transparency:** Set an example of direct and clear communication with stakeholders
- **Movement Building**: Inform and warn others of recent attacks tactics as well as lessons learned
- **Resilience Building:** Gain support and sympathy including more resources to address attacks
- **Push Back -- Go on the Offensive:** Use the attack to discredit opponents and build support for your work/issues/campaign/values. The attacks and bad actors should not be allowed to carry out their attacks without a response and ideally a full-on effort to stop or discourage them. They need to know there are consequences to attacks and "bad actors." Not responding may send a message that their attack(s) were successful in silencing or hobbling us.

Considerations: Are you ready to go public?

If you are funding social change organizations you should assume that it is likely that you will be criticized and attacked. Now is the time to engage in prevention and preparation measures so

that you are ready to face the storms. Conduct a risk assessment; and create a crisis management plan, which includes crisis communications strategies.

- Have you followed the WTS crisis management plan process for notification and response?
- Have you developed a clear and fact-checked narrative about the attack that discredits opponents and bolsters your credibility?
- If your foundation or one of your grantees has made a mistake or has a weakness exposed, have you prepared talking points that clarify the extent of the wrong and directly explain the corrective measures you/they are taking?
- Have you mobilized influential supporters including third party validators and close ally organizations to be ready to speak out on your behalf?
- Do you have personnel ready to accept, acknowledge and use support that is offered and needed?
- Have you taken steps to protect your most vulnerable stakeholders such as other designated spokespeople if your director is under attack?
- Have you removed all online contact information and/or created buddy systems or other security measures for people under attack?
- Have you assembled additional expertise and resources needed to defend the foundation or assist grantees under attack?
- Are you ready to respond to potential escalations of attack(s) as a result of going public?

Other Important Recommendations:

The following points, while not necessarily considerations regarding if/when to respond are important practices to adopt related to prevention, protection and future readiness.

- Have you asked grantees, peer and allies about their experiences so that you can monitor patterns of attacks?
- Have you designated resources and personnel to implement preventive measures? Have you built a culture of ongoing training and upgrading of practices to secure your people and your work going forward?

In closing, every attack requires an assessment and response plan. Doing your risk assessment, creating your Crisis Management Team and Plan, addressing internal vulnerabilities and creating a crisis communications plan will put your foundation in a strong position to 'weather the storm" and be able to support your grantees and the sector as a whole.

For more information, see https://roadmapconsulting.org/consulting-services/wts-public/ or contact info@roadmapconsulting.org.