

Newsroom Playbook for Propaganda Reporting

10 Guidelines

1

Develop newsroom social media guidelines—and require all reporters to abide by them. It is critical in these situations to fight the impulse to publish—or tweet—immediately. Commit instead to being first, responsibly. For example in the event of an extremely newsworthy hack, have the top editor send an organization-wide email instructing all staff not to live-tweet the content. Instead, indicate to readers that you are aware of the development and your reporters are working to determine the provenance of the material.

2

Remember that journalists are a targeted adversary and see yourself this way when digesting disinformation or hacks. Ask yourself: Are we being used here? Be on the lookout not only for obvious email dumps but also for direct messages sent via social media from dubious sources who may not be who they purport to be. Familiarize everyone in your newsroom with this minefield so they are aware of the risks.

3

Beware of campaigns to redirect your attention from one newsworthy event to another — and don't reflexively take bait. In 2016, the one-two punch of the Access Hollywood tape, followed less than 60 minutes later by Russia beginning the drip-release of John Podesta's emails, illustrated that news organizations want to be on high alert for stories intended to redirect the news cycle. This doesn't mean ignoring the late-breaking event; rather, it means covering the event in a manner that appropriately contextualizes the timing and substance of the event as potentially part of a disinformation campaign.

4

Break the "Pentagon Papers Principle:" Focus on the why in addition to the what. Make the disinformation campaign as much a part of the story as the email or hacked information dump. Change the sense of newsworthiness to accord with the current threat. Since Daniel Ellsberg's 1971 leak of the Pentagon Papers, journalists have generally operated under a single rule: Once information is authenticated, if it is newsworthy, publish it. How it was obtained is of secondary concern to the information itself. In this new era, when foreign adversaries like Russia are hacking into political campaigns and leaking material to disrupt our

democracy and to favor one candidate, journalists need to abandon this principle. That is not to say reporters ought to ignore the hacked material if it is newsworthy. But high up in the story they need to focus on the material's provenance. The why it was leaked as opposed to simply what was leaked. "You're in a whole different universe where foreign governments are trying to game the American democracy, especially the First Amendment privileges of the press, to benefit themselves and the candidate that they want to support," Taubman said. "And news organizations have to recognize that the Pentagon Papers Principle cannot apply in those cases. They have to have a different standard."

In other words, authentication alone is not enough to run with something.

5

Build your news organization's muscle for determining the origin and nature of viral information.

A responsible newsroom would never take the authenticity of leaked or other non-public content at face value because the authenticity of the content goes to the very heart of its newsworthiness. In the digital age, the same is increasingly true of provenance: the who, why, when and how of content's journey to the public domain may be an essential dimension of its newsworthiness. Establishing provenance, however, will in many cases require technical skills that few reporters possess. News organizations have options for filling this need, which range from establishing a dedicated, in-house digital provenance team with the necessary skills, to forming partnerships with other organizations to pool resources and build shared capability. The latter may sound like a stretch. But news organizations are already collaborating in areas like fact-checking.

6

Learn how to use available tools to determine origins of viral content. Reporters do not need advanced skills or degrees in data science to perform basic digital provenance analyses. Still lacking is a dream tool that could automatically tell reporters who first put something up on the Internet. But applications like [Hoaxy](#), [Graphika](#), [CrowdTangle](#) and [Storyful](#) help interpret trends and content on social media. The learning curve for these tools is not steep, and reporters who invest time in developing basic proficiency with them will often be able to develop a first-order approximation about provenance that could inform story development.

7

Be explicit about what you know about the motivations of the source and maintain that stock language in follow-up stories. Make sure that this guidance comes down from the top editors and is on a checklist of desk editors and copy editors so there are layers of oversight. There should be equal guidance to reporters who are active on social media that they prominently feature the provenance of the material and its goals in their distribution of this information. If the provenance isn't immediately known, focus your teams on answering that question. When there's a news imperative to cover a story, acknowledge that provenance is a question mark and explain in the story why the origin of the material is critical.


8

So the provenance doesn't get lost in follow-on stories or sidebars, consider having a box or hyperlink attached to every story on the topic with stock language reminding the reader of the motivation of the leak and why the news outlet is publishing the information. Extend this practice to any accompanying photos, videos or other content.

For example, stock language for the 2016 DNC hack reporting might have read something like this: "These emails were hacked by Russian operatives to undermine Hillary Clinton's campaign. The xxx is reporting on the portions that are deemed to be in the public interest and is refraining from reprinting those messages that are solely personal in nature."

9

Don't link to disinformation. If you do, make sure it is a no-follow link. We noted in our consultations with major news outlets that most are already independently deciding not to link directly to disinformation, an example of the kind of organic norm development that we seek to promote with this report. When news outlets link to disinformation, the content and its source (e.g. site, group or user) get amplified in people's feeds and in search engine algorithms. To avoid such amplification, refrain from linking to questionable content. Instead, describe the information with text and explain to the reader why you aren't linking to it. Alternatively, link to the content using a "no-follow link." Technologist Aviv Ovadya has explained how to do this in First Draft's report [here](#). Actions such as these signal to search engines to not count the link as a "vote" in favor of the target page's quality, which would improve its ranking and exposure. As Cornell Tech University expert on online information technologies Mor Naaman warns, however: "Remember that search engine and social media platforms may consider reader clicks on the link as a signal for interest, thereby contributing to the direct propagation of the



linked page.” For content that is authentic, he suggests, bring the file under your own domain name, instead of linking to a third party whose web platform and associated content you can’t control. This has the added benefit of drawing and keeping traffic on your site.

10

Assign a reporter to cover the disinformation/propaganda beat if you haven’t already.

Especially in the run-up to the election, having a reporter writing about information manipulation is recommended.