JULY 2024

INTERVENTIONS FOR ONLINE HARASSMENT OF JOURNALISTS

MOLLY CINNAMON

DESIGNED BY PRATIKA KATIYAR

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

Suddenly I was getting 100 tweets a minute. I'd open my phone at my kids' playgroup and see a picture of myself in a gas chamber."[1]

This is what Bethany Mandel, a conservative Jewish journalist, faced after publishing an article about former President Donald Trump's anti-Semitic following. In response, the police asked, "Why don't you just stop writing things on the internet that make people upset?"[2]

This unsympathetic reaction is precisely what the perpetrators of online harassment hope for. Online harassment of journalists aims to shape the broader civic conversation by limiting what can be said without destructive consequences. As more journalists are driven out of the public online sphere—or limit the scope or content of their coverage—due to harassment, one of the pillars of a free-thinking democracy is at stake: the freedom of the press.

This white paper aims to help address the problem of online harassment of journalists by identifying priority areas of technological, financial, or policy investment. The underlying research is rooted in workshops and breakout sessions with Berkman Klein Center for Internet and Society (BKC) affiliates who are experts in areas of technology, news media, law, and nonprofits. This white paper lays out these findings, identifying opportunities for cross-industry efforts that will multiply the protection of a single journalist into a network of press resiliency.

I. LIFESPAN OF JOURNALIST HARASSMENT ONLINE

Dogpiling – a coordinated effort to attack a target through "a barrage of threats, slurs, insults, and other abusive tactics"[3] – intends to silence the individual, punishing them for what they have published. This phenomenon is all too common: 73% of women journalists have experienced online harassment. In the face of such risks, 38% of women journalists have reduced their presence online, and 20% reported withdrawing offline altogether, self-censoring out of fear of online threats turning into offline violence. [4] These numbers do not even capture the totality of the problem. To determine how to disrupt dogpiling, the lifespan of harassment online must be understood: from the release of a journalist's work, to the inciting harassment incident, to the dogpiling itself, to the resulting chilling effect.

Figure 1: Lifespan of journalist harassment online.

Today, when a journalist's **work is released**, it often hits social media in tandem with publishing. The **inciting incident occurs** when trolls are catalyzed to harass the journalist, most often incited by a public figure (such as Tucker Carlson or Donald Trump) directing negative, vitriolic attention to the journalist or their work on traditional or social media.[5] Trolls use anonymous forums like Kiwi Farms or Doxbins to coordinate a **dogpile**, initiating a constant flow of harassing, threatening, and violent messages that utilize and dox personal information online about the journalist, their friends, and their family. Sometimes the online violence morphs into physical incidents, such as swatting or stalking. The **chilling effect** sets in when journalists do not publish again or limit the scope of their discourse due to the lasting psychological or reputational harm once the dogpile has died down. This is exactly what the dogpile participants want: to mold civic discourse, determining what can be said without reprisal.

II. TODAY'S LANDSCAPE: SOLUTIONS & BLOCKERS

Any new interventions to address the problem of online harassment of journalists should capitalize upon the existing valuable work done by nonprofit organizations, newsrooms, and technology companies. This section maps those solutions against the harassment lifespan, illustrating areas for growth due to existing limitations of policy, law, and economic realities.

1 *Story of Survival: Bethany Mandel, Online Harassment Field Manual*, Pen America (Mar. 30, 2018), https://onlineharassmentfieldmanual.pen.org/stories/bethany-mandel-editor-and-columnist-new-jersey.
2 *Id.*
3 *Defining "Online Abuse": A Glossary of Terms*, Pen America, https://online-harassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms (last visited Jan. 18, 2024).
4 *Id*. at 12.
5 The Chilling: A Global Study of Online Violence Against Women Journalists, International Center for Journalists 13 (Julie Posetti & Nabeelah Shabbir, eds. 2023) [hereinafter The Chilling]. https://www.icfj.org/sites/default/files/2023-02/ICFJ%20Unesco_TheChilling_OnlineViolence.pdf.

i. Pre-Inciting Incident: Limiting online exposure

Once a dogpile is underway, it is nearly impossible to stop. Thus, the most effective existing solutions are preventative. **Digital safety trainings** offered by nonprofits, well-funded newsrooms, and technology companies enable journalists to limit their online exposure and thus minimize fodder for harassment and doxing. For example, the nonprofits the International Women's Media Foundation (IWMF) and the Committee to Protect Journalists (CPJ) offer trainings for journalists to protect their data online and ensure device and communications security. CPJ's Digital Safety Kit even includes an editor's checklist to protect staff and freelancers against online abuse.[6] As a technical solution to this problem, the browser extension Privacy Party prompts social media users on how to lock down their accounts to maximize social media safety and reduce the content that can be weaponized against a journalist.[7]

While journalists can be guided to manually scrub their social media profiles, they lack control over the personal information accumulated by data brokers, including their email addresses and phone numbers. **Content removal services**, such as DeleteMe[8], PrivacyPros[9], and Optery[10], enable the continuous deletion of this data at a price ranging from roughly $50 to $300 a year, depending on their thoroughness. Although these services are not a panacea—content removal requests are not enforced by law—they reduce a journalist's potential attack surface.

BLOCKER: UNEVEN DEPLOYMENT

Digital safety trainings and content removal services are valuable only if they are used. Unfortunately, many newsrooms and journalists are unaware of preventative resources, even if free. Often, a journalist only becomes aware of the amount of their online exposure because they have been harassed. Once dogpiling occurs, reducing information online is significantly less effective—once an address or phone number is circulated on social media or forums, the journalist has nearly no control over its removal. In the face of the risk of online abuse and a lack of understanding about effective solutions, some newsrooms simply tell journalists to avoid discussing controversial topics online altogether.[11] But in doing

6 *Digital Safety Kit*, Committee to Protect Journalists, (Jul. 30, 2019), https://cpj.org/2019/07/digital-safety-kit-journalists; *Editors' Checklist: Protecting Staff and Freelancers against Online Abuse*, Committee to Protect Journalists, (Jul. 7, 2022) https://cpj.org/2022/07/editors-checklist-protecting-staff-and-freelancers-against-online-abuse.
7 *Introducing Privacy Party*, Block Party App (May 30, 2023) https://www.blockpartyapp.com/blog/introducing-privacy-party.
8 *DeleteMe*, https://joindeleteme.com (last visited Jan. 18, 2024).
9 *PrivacyPros*, https://privacypros.com (last visited Jan. 18, 2024).
10 *Optery*, https://www.optery.com (last visited Jan. 18, 2024).
11 The Chilling, *supra* n.8 at 14.

Point in Lifespan	Current Solution	Solution provided by	Solution implemented by	Blockers
Pre-Inciting Incident	Limiting online exposure—social media lockdown	Nonprofits, newsrooms, technology companies	Journalists	Lack of awareness, often not actually completed before the inciting incident
Pre-Inciting Incident	Limiting online exposure—data broker content removal	Technology companies, newsrooms	Journalists, newsrooms	Cost, uneven deployment
Dogpiling	Guidance during the dogpile: digital security & logging	Nonprofits	Journalists	Lack of awareness, lack of access to digital expert
Dogpiling	Physical security & online security	Newsrooms, Nonprofits	Newsrooms, Technology Companies	Cost, often done too late, unsteady reliance on platforms
Dogpiling	Escalation Channels	Technology Companies	Technology Companies	Fickle, high reliance on platforms
Chilling Effect	Communities for mental health recovery	Nonprofits	Journalists	Lack of awareness, may be too late

i. Current solutions and blockers

so, the press does the dogpilers' work for them, undercutting its own freedom out of fear of harassment.

ii. During Dogpiling: Guidance & Efforts for Safety

Once dogpiling starts, well-funded newsrooms and nonprofits offer a patchwork of mitigating tactics. **Digital security and logging** efforts can help journalists respond to an ongoing attack and seek assistance from law enforcement, security experts, and platforms. For example, AccessNow's Digital Security Helpline provides incident response-based guidance to journalists on how to manage privacy and cybersecurity concerns in the wake of a dogpile.[12] Nonprofits RaReNet (Rapid Response Network) and CiviCERT have created the Digital First Aid Kit, guiding journalists on how to log evidence of attacks for technical and legal help.[13]

Well-funded newsrooms have some resources at this stage of harassment. When online harassment crosses over into in-person threats or actual violence, some newsrooms may offer **physical security** resources, including relocating a journalist during a period of in-person harassment after being doxed. They may also use informal **escalation channels** to contact Trust and Safety teams at social media platforms to expedite a response to their takedown requests of harassing content. Facebook, TikTok, and the Twitter (as it was known before Elon Musk's takeover)[14] use a "Trusted Partners" system to engage with civil society organizations such as AccessNow. These relationships can enable informal escalation channels to raise urgent content removal requests.

BLOCKER: COST & FICKLE RELATIONSHIPS WITH SOCIAL MEDIA PLATFORMS

These tools have mental and economic costs. Digital security and logging efforts, while highly valuable, still require journalists to be the first responders to their own harassment—receiving the vitriol, blocking trolls, and managing their online presence.[15] As for security solutions sustained by news outlets, those costs are likely out of scope for smaller shops. And even in large, well-established newsrooms, not all employees are full-time; many are contributors or freelancers who would not get the benefits of such protections.

Changing relationships with platforms have created uncertainty about solutions that rely on their cooperation. Given recent Congressional and political scrutiny of social media platforms and content removal,[16] platforms are cautious about opening up informal escalation channels that could be criticized as perpetuating "censorship." Even in the absence of such scrutiny, purely relationship-based escalation channels are innately vulnerable; if those contacts leave, are fired, or laid off, or even just reassigned within the company, those channels are closed. Additionally, some social media platforms have made interoperability with their technology unreliable; when Twitter shut off free access to its API in April 2023,[17] many critical technologies mitigating harassment on the site became defunct. For example, the plug-in Block Party (by the same creators as Privacy Party) relied on Twitter's API to enable users to shield themselves from harassment by mass-blocking users or filtering out certain content. Without reliance on APIs, much platform-enhancing technology to protect journalists from dogpiling cannot be built.

iii. Preventing the Chilling Effect: Community-Building

To preserve journalists' mental health and prevent them from leaving the industry, nonprofits suggest forming communities to share the emotional burden with others similarly affected.[18] Beecause public presence poses the risk of infiltration by trolls, these communities often require a direct introduction by a nonprofit or other journalist in-the-know.

12 *Digital Security Helpline*, AccessNow, https://www.accessnow.org/help (last visited Jan. 18, 2024).
13 *Documenting Digital Attacks*, Digital First Aid Kit, https://digitalfirstaid.org/documentation (last visited Jan. 18, 2024).
14 This memo will refer to the service now called "X" as "Twitter" for consistency's sake.
15 The Chilling, *supra* n.8, at 26.
16 *See, e.g., 'Twitter Files' authors testify before House Judiciary Committee* (Nov. 30, 2023), https://thehill.com/homenews/4335249-twitter-files-authors-testify-house-judiciary-committee-watch-live.
17 Matt Binder, *Twitter Cuts Many App Developers' API Access, Even Those Willing to Pay $42,000 per Month*, Mashable (Apr. 4, 2023) https://mashable.com/article/twitter-cuts-off-api-access-apps.
18 *See e.g., Finding Supportive Cyber Communities: Online Harassment Field Manual*, Pen America, https://onlineharassmentfieldmanual.pen.org/establishing-supportive-cyber-communities/ (last visited Jan. 18, 2024).

BLOCKER: LACK OF LEGAL RECOURSE

Yet, for a journalist hoping to obtain affirmative recourse, the United States' strong free speech protections, combined with the anonymous nature of most online accounts, make it difficult for journalists to go on the offensive against a dogpile. Litigation costs against hard-to-find and likely judgment-proof defendants comprise a barrier to entry for individual journalists and many news outlets, and the difficulty of winning defamation suits—especially when journalists themselves can be considered public figures—may mean there is no vindication at the end of the process. Platforms too are shielded from nearly all liability, even for actionable content, by Section 230. Thus, unless this legal gridlock changes, near-term efforts to reduce journalist harassment online must come from sources other than the law.

III. PROPOSED INTERVENTIONS

Informed by subject matter experts, the proposed interventions aim to halt progression in the online harassment lifecycle, ultimately subverting the chilling effect.

i. Trust & Safety Co-op

A Trust and Safety Co-op, consisting of Trust & Safety (T&S) professionals from various platforms, could enable a structured mechanism for anticipating, identifying, and halting dogpiling across the Internet. Because harassment rarely stays on one platform, T&S teams should harness their collective knowledge to inform awareness of ongoing or future harassment. Information sharing may be as simple as publishing alerts of dogpiling underway or as complex as sharing analytical tooling to predict when a dogpile is likely to occur. In response, T&S teams can apply their respective platforms' policies to the content. But by working from a collective knowledge base, T&S teams can lower the risk of dogpiling on multiple platforms.

NEED: ORGANIZATION

Appropriate governance and transparency is an existential requirement for a T&S Co-op. As described previously, opaqueness and informality risk distortion of a collaborative effort, falling into the political trap of being labeled as an effort for "censorship." Transparency helps fight this narrative. For example, the creation of Meta's Oversight Board and its publication of transparency reports have been used to respond to concerns about Facebook's uneven content moderation. While not a permanent fix to a public perception issue, accountable governance has staved off cries of censorship. A T&S Co-op should follow suit.

ii. Journalist Co-op

A Journalist Co-op, consisting of freelance journalists and journalists from small, under-resourced news outlets, would enable the pooling of resources to achieve the same protections from harassment as those at major, well-resourced news outlets.

Proactive online security is the most critical defensive tactic in the face of online harassment. This co-op would help every single member journalist lock down their social media profiles and enact strong cybersecurity protections, ideally before publishing their first story. For example, this co-op could form a mutually beneficial partnership with Privacy Party, the free browser extension that automatically locks down users' social media settings: in ensuring that as many journalists as possible use this tool, the overall attack surface for online harassment would be minimized, and Privacy Party could expand their user base.

Full benefits of membership in the co-op should be gated based upon whether the journalist has taken free prescribed protective measures. Upon full membership, the co-op could fund a journalist's subscription to data broker content removal services, connect them with digital experts, and provide them with funds for physical security in the event of severe doxing.

NEED: FUNDING

Protecting journalists is expensive. For example, personal-data removal subscriptions are pricey for one journalist, let alone for hundreds or thousands of journalists. To incentivize use of these protective technologies, this co-op could broker a deal between news outlets and Media Liability insurers: news outlets which provide their journalists with proactive privacy tooling should receive lower insurance rates, as such tools are likely to reduce a news outlets' risk of liability when a journalist suffers from harassment. Additionally, pro-bono partnerships with the companies behind these proactive technologies would make their protections widely deployed.

iii. Tool for Automated Harassment Reporting

A tool to automatically compile digital evidence of online harassment would enable journalists to more easily obtain aid from platform T&S teams, digital security experts, and law enforcement. The tool would sweep journalists' multiple social media

accounts for harassing posts or messages, then compile and share the collected content into databases or reports, depending on the preferred mode of input for each receiving party. To prevent the need for manual review, targets of harassment could tag a few posts as indicative of the harassment, and artificial intelligence and natural language processing tools could be used to infer other posts within the same dogpile. If the journalist was willing to provide personal information like phone number and address, the tool could flag doxing content. An automated tool not only makes the process of reporting for platform, cybersecurity, and legal help easier, but it reduces the risk of a journalist slipping into a chilling effect because of the psychological burden of reviewing their own harassment.

NEED: TECHNICAL & LEGAL RESEARCH

Any technical intervention built on top of platforms, including an automated reporting tool, must overcome the lack of API access to the platforms. In the face of this obstacle, some developers have pivoted to building browser extensions to create middleware-like functionality for their users. A browser extension executes with the authority of the user and simply scripts on top of the site the user visits. For example, after Block Party was shut down due to Twitter rescinding free API access, founder Tracy Chou pivoted to creating Privacy Party as a browser extension.[19] While scripting does not enable the same automated and mass data pulls as APIs, browser extensions are a valuable work-around to existing limitations. Still, more research is needed to expand the possibilities of how independent safety tools can be built without reliance on platforms. For example, can browser extensions be built to run on mobile, or even run tasks in the background (with user permission)? Could phone apps be written to access the local copy of social media content other apps load onto the device? Solving these technical problems would unlock a range of new tooling to mitigate online harassment. But a new technological workaround creates new legal concerns. Certain end-user license agreements (EULAs) may prevent scripting over certain apps for certain purposes. To build browser extensions and scripting services that can reliably scale, more technical and legal research is needed to determine the limits of those technologies.

19 Block Party's Twitter Product is on Indefinite Hiatus as of May 31, Block Party App (May 30, 2023), https://www.blockpartyapp.com/blog/twitter-hiatus.

Point in Lifespan	Intervention	Goal	Solution enabled by	Resource need
Inciting Incident	**Trust & Safety Co-op**	cross-platform collaboration to anticipate and halt dogpiling—while ensuring **appropriate & transparent governance**	Social media platforms T&S teams, academia, nonprofits	Funding, organization of existing efforts, buy-in from T&S teams
Pre-Inciting Incident, Dogpiling	**Journalist Co-op**	provide **all journalists** with the same **protections as well-funded news outlets**	Nonprofits, newsrooms	Funding, organization, buy-in from journalists and news outlets
Dogpiling	**Automated reporting tool** for harassed journalists	Auto-capture instances of harassment for **platform, law enforcement, and digital security documentation**	Technologists, journalists	Technical skill, resourcing, organization
Dogpiling, Chilling Effect	**Further research** for online harassment of journalists	**Reporting dashboard** illustrating ongoing trends of online harassment	Collaboration between technologists, journalists, nonprofits	Funding, organization, technical skill

Near-term interventions: level up existing solutions

iv. Reporting Dashboard Tracking the State of Harassment

Anecdotal stories of harassment have done critical work in raising public awareness of dogpiling. Currently, however, there is a missed opportunity to drive change by transparently collecting, studying, and presenting the full data from the many dogpiles that happen every week, month, and year. Upon obtaining a journalist's consent, researchers should continuously pull data from their social media feeds into a "data observatory," a database of all content from all feeds from all participating journalists. From this data observatory, natural language processing and other models can be run to observe what posts spike harassment, how dogpiling evolves, and how abuse impacts journalists over time. The data can be used to create a live reporting dashboard to drive awareness and put pressure on social media platforms to respond to this issue, as well as fuel research about the very nature of online harassment.

NEED: BUY-IN & TECHNICAL RESEARCH

This research requires collaboration between journalists, academics, technologists, and data scientists. Developing an accurate, apolitical data observatory of online harassment of journalists requires buy-in from many journalists across political lines. And the stakes are high: if personal data from the research is leaked, harassment against these journalists (and the researchers who compiled the data) could begin with a renewed vigor. Additionally, such research would butt up against aforementioned limitations on API access. API workarounds, such as browser extensions, are a prerequisite to obtaining data inputs for research.

i. Enable Middleware to Unlock Third-Party Development

Cost-effective API access is critical to building technology that combats harassment. For example, tooling that is interoperable with social media platforms can automatically lock down a journalist's online presence, enforce the strictest cybersecurity controls, and create content filters to minimize exposure to dogpiles. Such automated tooling would increase the broad implementation and efficacy of privacy and cybersecurity controls many times over. Simply restoring API access at Twitter would revive valuable tools such as Block Party.

Without government regulation, platforms do not have a strong market incentive to provide affordable API access. Change will only come with regulation, and those changes are slow moving. Federally, the agent of change may be antitrust regulation, breaking apart companies or at least requiring interoperability.[20] In 2021, the FTC sued Facebook for anti-competitive practices, in part for closing off API access to third-party developers producing tooling similar to Facebook or connecting to other social media platforms.[21] The viability of this claim and resulting damages remain to be seen; the case is ongoing. In states, the momentum of privacy legislation should be used to fuel interest in legislation for open APIs. The New York State Senate has led the way, proposing a bill requiring social media applications to maintain an open API accessible to third-party platforms.[22] Funding is needed to continue fighting this fight, even if piecemeal at the state level.

ii. Pass Privacy Legislation to Reduce Online Exposure

Today, it is nearly impossible for an American online to track all of the public sites on which their data is listed. Even for someone with every proactive privacy protection in place, personal information can still be in circulation online, enabling doxing and stalking. In the absence of federal legislation,

20 Asher Schechter, Filippo Lancieri, *"A Loaded Weapon": Francis Fukuyama on the Political Power of Digital Platforms*, ProMarket (Dec. 4, 2020) https://www.promarket.org/2020/12/04/francis-fukuyama-political-power-digital-platforms-middleware.
21 Complaint, *Federal Trade Commission v. Facebook, Inc.*, No. 1:20-cv-03590 (D.C.C. Jan. 13, 2021).
22 Proposed Senate Bill S6686, State of New York, https://www.nysenate.gov/legislation/bills/2023/S6686.

"DEVELOPING AN ACCURATE, APOLITICAL DATA OBSERVATORY OF ONLINE HARASSMENT OF JOURNALISTS REQUIRES BUY-IN FROM MANY JOURNALISTS ACROSS POLITICAL LINES. AND THE STAKES ARE HIGH: IF PERSONAL DATA FROM THE RESEARCH IS LEAKED, HARASSMENT AGAINST THESE JOURNALISTS (AND THE RESEARCHERS WHO COMPILED THE DATA) COULD BEGIN WITH A RENEWED VIGOR."

state privacy laws must continue to expand consumers' data rights and limit the reach of data brokers. For example, California passed the Delete Act at the end of 2023, putting legal teeth into the removal requests made on data broker sites.[23] To put collective pressure on the industry to conform with privacy-preserving standards, more states need to pass laws of this nature. Still, much personal information used to fuel doxing and in-person harassment, such as residential addresses, can be found in public records, including property transactions and voter registrations. States and the federal government alike need to look more closely at the privacy and security concerns generated by online access to public records while balancing transparency interests.

iii. Expand Harassment Laws to Encompass Online Threats

State laws against harassment need to be evaluated and amended to ensure they provide protection for those experiencing online threats and related in-person stalking, both symptoms of dogpiling. Across all states, restraining orders are most commonly granted in cases of domestic and intimate partner violence,[24] and judges are hesitant to grant orders that may restrict freedom of speech. For these reasons, journalists experiencing harassment online may have a difficult time convincing judges to extend their interpretation of harassment laws to credible threats and abuse from an online-only, non-interpersonal relationship. State laws must be tweaked to ensure they respond to an era in which online communication is a major medium for harassment.

IV. CONCLUSION

In today's age, journalists face an impossible choice: publish groundbreaking truths on socially-critical issues and face seemingly endless harassment and threats, or forgo publishing altogether, saving themselves and their family from becoming the targets of online and offline violence. The interventions proposed in this white paper aim to eliminate this choice, or at least make it significantly easier, by undermining the effectiveness of the dogpile. If successful, journalists could publish freely, and freedom of the press would be protected. Critically, the impact of these proposed interventions would benefit more than just journalists. The co-ops, tools, and legal changes recommended in this white paper would give all individuals online tools to proactively and reactively respond to online harassment. By elevating existing solutions and harnessing collective power across industries, we can disrupt the dogpile and empower speech without reprisal—for journalists and anyone online.

24 *Restraining Orders & Online Harassment: Online Harassment Field Manual*, Pen America, https://onlineharassmentfieldmanual.pen.org/restraining-orders-online-harassment (last visited Jan. 18, 2024).

Point in Lifespan	Solution	Goal	Solution impacts	Resource need
Pre-Inciting Incident	**Regulations to force API access**	Enable research & technical solutions to **automatically minimize online presence and enforce strong cybersecurity controls**	Platforms, technologists, researchers	Policy change, technical skills, organization
Pre-Inciting Incident	**Privacy legislation**	**Reduce** the amount of uncontrollable **personal information online**	Journalists	Legal change
Dogpiling	**Harassment law reform**	Amend state laws for protective orders to ensure they provide **recourse in dogpiling**	Journalists	Legal research, legal change

Long-term interventions: shape policy & law to unlock new solutions

INTERVENTIONS FOR ONLINE HARASSMENT OF JOURNALISTS SUMMARY

Online harassment of journalists poses a grave risk to press freedoms: retaliating in response to a disfavored article or post, trolls coordinate abuse in the hopes of silencing the journalist altogether. To protect journalists from this outcome, this white paper provides recommendations for interventions to interrupt the lifespan of harassment online. These recommendations are informed by a literature review, review of existing solutions, and interviews with stakeholders in areas of technology, news media, and nonprofits.

Recommended interventions that can be deployed near-term

- Trust & Safety Co-op: a community of T&S professionals empowered to share predictive analytics and reports of ongoing harassment, helping stop online harassment earlier
- Journalist Co-op: a community of journalists centered around resource-sharing, ensuring every journalist is equipped with tools to respond to harassment proactively or reactively
- Automated Harassment Reporting: a tool to automatically collate instances of harassment across platforms, allowing journalists to more easily secure aid from trust and safety teams, digital security experts, and law enforcement
- Public Reporting Dashboard: live metrics of journalist online harassment to apply public pressure to social media platforms, prompting their attention on this issue

Recommended interventions requiring longer-term investment

- Open API Access: policy change to force platform interoperability for third-party developers, enabling them to build tools to mitigate online harassment
- Privacy Legislation: legislation to enable journalists to exercise control over their personal information online, such as wiping their information from data brokers
- Expanded Harassment Laws: policy recommendations to ensure that state protective orders cover dogpiling-spurred harassment, not just domestic violence situations

These recommendations provide ready-to-deploy means to protect journalists from online harassment, ultimately providing a path forward to protecting freedom of the press.