GIJN Toolbox: Cutting-Edge — and Free — Online Investigative Tools You Can Try Right Now

by Rowan Philp • March 13, 2024 ⋮ 9-11 minutes

The 2024 NICAR data journalism summit — hosted in Baltimore by Investigative Reporters and Editors — surfaced scores of innovative reporting resources and tools, primarily for US data reporters.

Image: NICAR 2024

GIJN curated these tips and databases for ones that are transferable to investigative and data reporters around the world, and we will share these globally relevant techniques in several stories in the weeks to come.

In this first story from NICAR24, we highlight some new, free investigative tools on fact-checking, topic briefing, and journalist safety that were the subject of significant interest in the hallways at NICAR, and which could help reporters in almost any country right now.

New Google Tools for Quickly Investigating Images

'About This image.' This is a brand new feature that can help journalists check the general history of an image in seconds. Having selected a picture in Google Images, simply click on the image, then click on the three vertical dots alongside — and then select the new "About this image" tab. The tool immediately shows roughly how long the image — or even a similar image — has lived on Google, and can immediately debunk claims that it was newly captured. It sometimes also offers useful information from metadata, including notes on any AI enhancement.

Fact Check Explorer. Has a suspicious claim or image you've encountered already been verified or debunked by a vetted fact-check organization? This new Google interface is a search engine exclusively for verified fact checks and allows reporters to get a quick summary of the verdict as well as a link to the original verification report.

"These results are all from reputable news or fact-check organizations, so you shouldn't find any misinformation in this tool except for those claims that have been fact-checked," said Mary Nahorniak, US teaching fellow at Google News Initiative. "What I like is that you see the claim, but it's always married to the result."

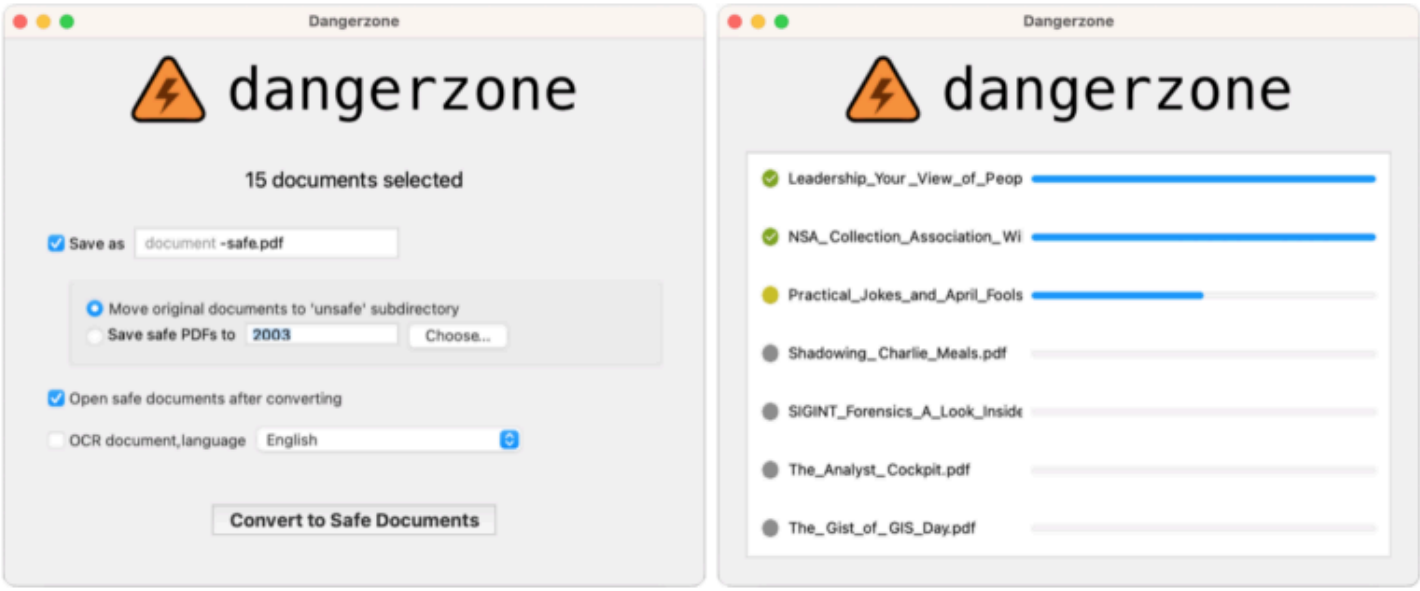
Image Search Beta and Google Image Context. Reporters can fill out a simple form to apply for access to this new tool, which pulls up all fact checks done involving the picture you upload. It works on the image itself, rather than the metadata — so even uploaded screenshots of a suspicious image can work. But perhaps the most powerful feature of Image Search Beta is its Image Context feature,

which tells you the exact day on which the image was first indexed, as well as other details of its origins.

“This kind of tool did not exist till a few months ago — before, you had to reverse image search and then sort by time, and go back til you no longer saw it,” Nahorniak explained.

Dangerzone Tool Scrubs Malware from PDF Leaks

Investigative sources leaking information in electronic document form sometimes unwittingly pass along dangerous malware — and bad actors have also been known to attack newsrooms with deliberately infected “news tips.” Hosted by the Freedom of the Press Foundation — and needing just one click — the open source Dangerzone tool makes a copy of the document you upload to the tool that excludes the bugs and converts the document into a safe PDF. It also parks the original document in a place where you won’t accidentally open it, and creates a “virtual computer” for the upload as added protection against aggressive or exotic malware.



The Freedom of the Press Foundation created the Dangerzone tool to screen out any potential malware from whistleblower-leaked documents. Image: Screenshot, Dangerzone

“This was designed with journalists in mind, and it takes your PDF — which might be spicy with malware — and makes it safe,” explained David Huerta, a senior digital security trainer at Freedom of the Press Foundation. “It can also do some OCR (optical character recognition) functions.”

Note that there are other PDF security threats that it does not address — such as the threat of markings that are sometimes covertly added to confidential documents to expose potential whistleblowers. “If you’re worried about privacy implications of what’s on the document itself, like printer dots or intentional misspellings, it won’t catch that, because it’s making a visual copy of the PDF,” Huerta acknowledged.

Perplexity AI ‘Answer Engine’ for Initial Briefings on Complex Investigative Topics

Like answers from all AI chat tools, those from Perplexity.ai need to be carefully verified, or used as leads rather than evidence. But this new tool impressed many experienced investigative journalists at NICAR 2024 as an excellent briefing tool, in particular — especially for watchdog reporters tackling a complicated, unfamiliar subject. Perplexity is a new kind of search engine that – rather than spitting out a list of website links from keywords — provides concise responses to complex investigative questions, as well as curated lists of authoritative sources and insightful suggested follow-up questions.

Drill deeper, its early users say, and it tends to take you where *you* want to go, rather than where *it* wants to take you. While not a direct source of verified data — and relying on large language model (LLM) AI — this so-called "answer engine" was recommended by Jeremy Caplan, director of teaching and learning at the CUNY Graduate School of Journalism, as a unique and quick way to brief reporters on new investigative subjects and potential leads. It also has a powerful free dashboard with the option of paid-for upgrades.

"Understanding complexity is important for reporters — anyone can search Google, which will give you a hundred links. But Perplexity gives you the ability to understand complex questions, with citations and relevant onward questions," said Caplan. "There is the potential for there to be other tools for this, but Perplexity is the one I'd recommend right now. It's beautifully rendered — it gives very specific examples, and it's a very useful tool for quickly getting up to speed."

Asked about money laundering techniques popular in Eastern Europe, the tool offers 10 distinct methods — from "smurfing" and bulk cash smuggling to layering and trade–based laundering — as well as summaries and links to recent investigative stories on the topic.

Caplan added: "What I really like is that it offers a series of questions to follow-up on. You gradually gain a richer and richer understanding of a subject, while retaining the ability to verify at any stage."

Asked, for instance, "How does timber trafficking in the Amazon work?" Perplexity offers a detailed and contextual summary — with citations of work by Mongabay, Earth Restoration Service, and Corporate Accountability Lab — as well as three linked, follow-up questions. Drilling down into one of those questions reveals a handy list of the countries that purchase the most furniture made from trafficked Amazonian timber, with links to sources such as Greenpeace reports. This is a must-try tool for small newsrooms in the Global South.

PrivacyPartyApp to Guard Against Harassment and Doxxing

The main reason most journalists don't select the right privacy settings on the many social media platforms we use is not that we can't figure them all out, but rather that we just don't have the time or bandwidth to do all of this. For instance: simply updating the privacy level of a photo album on Facebook normally takes six manual clicks, and a lot of time to figure each click. But the threat of doxxing and harassment of investigative reporters — and especially gendered harassment — is severe, and growing.

Created by Block Party, the PrivacyParty app scans your settings and offers recommendations. It not only finds and clicks all your preferred privacy settings for you, but also concisely explains the privacy-versus-access trade-offs for each before you click its "Update" tab — and it constantly updates itself for new threats. Essentially, it is a virtual "IT help desk" standing over your shoulder, only it works much faster. To use it, you need to create an account, download the browser extension, and choose your platforms. The app currently works on Facebook, LinkedIn, Twitter (X), Strava, Instagram, and Reddit, and its developers regularly add new platforms.

The PrivacyParty service is currently free, as it is still in beta form. Note, it is currently available only for desktop, rather than mobile.

"It's kind of annoying to have to know all of the platforms and their potential risks, all the settings you have to pay attention to, and the trade-offs you're willing to accept, and nobody wants to wade through all the horrible UX of all these settings," said Block Party CEO Tracy Chou. "It's just tedious. PrivacyParty will walk you through the platforms, the settings and trade-offs, and once you decide you want to take an action, we'll go through the task of navigating them and update them for you."'

Chou conceded that oligarchs and other bad actors could potentially use PrivacyParty to hide reporting vectors to their public posts on social media, but said that "more advanced methods reporters use to find them would still be available."

Rowan Philp *is GIJN's senior reporter. He was formerly chief reporter for South Africa's Sunday Times. As a foreign correspondent, he has reported on news, politics, corruption, and conflict from more than two dozen countries around the world.*