

Tow Center for
Digital Journalism

Guide to Information Warfare Reporting

October 2026

This research is generously funded by the Tow Foundation and the John D. and Catherine T. MacArthur Foundation.



TOW CENTER
FOR DIGITAL
JOURNALISM

Table of contents:

<u>Introduction</u>	3
1. <u>A Brief History of Information Warfare</u>	7
2. <u>“Who’s Behind This Website”: Tricks and Tips for Digital Investigations</u>	16
3. <u>Q&A: Martin Vassilev on scams, bans, online hustling, and playing cat and mouse with the big tech platforms</u>	31
4. <u>Infowars in America: Hoaxes, Propaganda, and the War on Rumor</u>	39
5. <u>Q&A: Researcher Danielle Tomson discusses her experiences studying MAGA influencers, pre-bunking social media falsehoods, and the difference between rumors and disinformation</u>	48
6. <u>A Reporting Guide to AI-Generated Intimate Images</u>	56
7. <u>Q&A: Brandy Zadrozny on Conspiracy Theories, Protecting Sources, and Protecting Herself from a “Depressing” Beats</u>	63
8. <u>The Other Side of the Recorder</u>	70
9. <u>Q&A: The Insider’s Michael Weiss on war reporting, intercepted data, and the perils of investigating foreign intelligence services</u>	75
10. <u>Q&A: “It’s a game changer.” Allie Funk on AI, human rights, and digital surveillance</u>	82

Edited by Stuart Anderson-Davis, Michael H. Keller, and Vicky Walker.

Introduction

By Professor Emily Bell and Michael Henry Keller

Emily Bell is the Leonard Tow Professor of Journalism and Director of the Tow Center for Digital Journalism at Columbia Journalism School. Emily was a business reporter and editor, covering media, technology, and advertising. Before joining CJS in 2010 she led the editorial development of The Guardian’s websites, podcasts, and newsletters. The Tow Center is known for its groundbreaking work in tracing the relationship between big tech companies and journalism, and developing the field of computational journalism.

Michael Henry Keller is an investigative reporter at The New York Times. His reporting focuses on the intersection of technology and society, covering topics such as artificial intelligence, policing, surveillance, and online child safety. His work combines a traditional investigative approach with computational techniques to produce human-driven stories backed by rigorous, data-driven foundations.

Emily and Michael co-teach the Information Warfare Reporting class at Columbia University’s Graduate School of Journalism.

Canadian communications scholar Marshall McLuhan predicted in his 1970 book [*Culture Is Our Business*](#) that “World War III” would be “a guerrilla information war with no division between military and civilian participation.” Few media predictions seem so likely to be realized — especially not those made over fifty years ago, long before the rise of AI and social media. At the most basic level, “information warfare” involves the use of tactics that exploit the information environment to the detriment of particular societal groups within society, or even against whole populations.

In her 2018 paper [“Information Warfare: Issues for Congress,”](#) national security expert Catherine A. Theohary writes that information warfare is conducted “not only in crisis, conflict, and warfare in the operational sense, but is ongoing in peacetime as well.” As she notes, whatever the target (“government agencies, political leadership, or news media”), the goal is “to influence public opinion or to compel decisionmakers to take certain actions” as “ultimately the target of information warfare activities is human cognition.”

We introduced an information warfare reporting class for students at Columbia Journalism School in 2020. It was clear at the time that reporters and journalists were on the frontlines of the information war, both as targets and as narrators. Journalism schools traditionally prepare students for operating in

physically hostile reporting environments, including conflict zones, but little time is devoted to preparing journalists to work in hostile *information* environments.

Often these two arenas overlap, as we have seen in the targeting of journalists working in Gaza, Ukraine, Russia, Iran, Sudan, Yemen, the United States, and elsewhere. Beyond the deadly physical threats that journalists face — augmented by online security threats and harassment — every reporter on any beat, from the local school board to global diplomacy, must develop a sophisticated understanding of the media environment in which they operate.

As so much of this space is mediated through the internet, where commercial incentives drive parties to capture user attention and harvest user demographics — an understanding of data collection and uses is key. This can take the form of neighborhood Flock cameras, a new health-tracking app, or Generative AI models and social media platforms. Each can be designed with vulnerabilities and biases; viewing them through the lens of information warfare means examining who is shaping them, for what purpose, and how those who benefit are held accountable, if at all.

This guide is a compilation of essays, resources, and interviews with practitioners in the field. Each has taken the time to visit our class, engage with our students, and share their stories and expertise. We are incredibly grateful for their insights and support.

Over the past seven years, the field has been a target-rich environment: Covid, the January 6 insurgency, Elon Musk buying Twitter, the introduction of Generative AI tools, the latest wars in the Middle East and Ukraine, and ICE using surveillance technology on US citizens. Our students have tackled many of these events as they've unfolded, including exposing [gunmakers marketing their deadly products to extremists on social media](#); uncovering evidence of [self-dealing and fraud by a Trump appointee and right-wing personality](#); reporting on how [conspiracy theories and election denialism shape the views of people in New York](#); and revealing [how trans people were often scapegoated in the wake of national tragedies](#).

But as technology rapidly evolves, the core of reporting remains the same as it has always been: identifying and interviewing the right people. Our students often talk to reluctant subjects: sometimes those who operate at the edges of legality and those who might themselves be vulnerable and need protection.

This beat is growing. Major newsrooms have developed sophisticated data and visual investigations desks and hired more reporters covering technology as a human rights issue. There's a heartening array of in-depth independent reporting. Anyone who follows the work of [404 Media](#) or Craig Silverman's [Indicator](#) will get a sense of the type of stories that make up this diverse beat. If you want to dig deeper into the world of online crime, there's the [Darknet Diaries](#) podcast. Online publications like [Coda](#)

[Story](#) cover the effects of technology companies' actions outside the United States. The use of AI and surveillance systems in war and genocide are documented to devastating effect by the reporting of [+972 Magazine](#), which grew into the *NAZA* documentary. The guide is not exhaustive, but provides background on core areas we focus on in class.

Information warfare is a field filled with confusing and ever-changing jargon. In our first piece, Columbia Journalism School doctoral researcher Stuart Anderson-Davis explores some of the key concepts and case studies that show how information warfare has shaped events and manipulated audiences over the centuries.

New technologies and trends are readily exploited in this area. In a joint piece packed with useful links and resources, investigative data journalist Jon Keegan, who started the course with Emily in 2020, and Priyanjana Bengani, a former Computational Journalism Fellow at the Tow Center for Digital Journalism, share their insights on investigating websites and platforms, including how to adapt research techniques in a rapidly evolving digital landscape.

One reporter who has shone light on the murky world of information warfare and darker sides of the internet is Brandy Zadrozny, a senior enterprise reporter for MS NOW. In our Q&A, Brandy discusses the importance of covering conspiracies and disinformation, including the personal toll of online harassment and engaging with disturbing content.

Not all information warfare is undertaken with intent to harm. What if the purpose is pure profit? Is it a crime to manipulate major tech platforms to make money and generate attention — or just a business model? This is a question explored in Michael's Q&A with Martin Vassilev, a digital entrepreneur he first met in 2018 when reporting on [fake YouTube views](#) for *The New York Times*. Here, Martin provides his firsthand perspective on online fakery in an age of AI and the thriving (but largely concealed) business of digital deception.

One scholar who has literally [written the book](#) on fakery is Andie Tucher, a prize-winning professor of journalism at Columbia University. In her essay, Andie explores the intertwined history of information warfare and the American press over the past 250 years. Andie identifies several key challenges faced by those attempting to better understand and address the effects of information warfare.

The danger of disinformation is a theme of our Q&A with Michael Weiss, an investigative reporter, author, and media commentator who specializes in war and espionage. He discusses the personal and professional threats he's faced over the years — from reporting from war zones and cultivating sources within the intelligence services to facing hacking attempts by foreign governments and coordinated trolling campaigns.

While information warfare operations may be mounted by nation states, they can also be perpetrated by individuals for a whole range of reasons, including highly personalised efforts to harm and humiliate an individual. In her article, Kaylee Williams — a Ph.D. candidate at Columbia University’s Graduate School of Journalism and lecturer in the Media Studies program at University of California, Berkeley — discusses the rise of sexually explicit deepfakes and AI-fueled “nudification” apps. Kaylee identifies the threats posed by this technology, and explains how reporters can cover this subject with more accuracy and empathy, while also protecting themselves and their colleagues.

The importance of reporting with empathy and care is a core theme of the essay by Anika Collier Navaroli, an award-winning writer, lawyer, and researcher. Anika shares her own experiences of becoming a whistleblower and what it was like to tell her story through the media. Now teaching the next generation of journalists at Columbia Journalism School, Anika offers important practical guidance for any reporter working with sensitive sources.

Personal experiences — and the value of taking time to truly engage and understand your subject — is a key takeaway from our Q&A with Danielle Lee Tomson, a writer, scholar, and strategist. Danielle discusses her work researching conservative social media influencers in America — including time spent alongside figures like Steve Bannon, Jack Posobiec, and Laura Loomer — while sharing her insights on how information warfare might shape the upcoming midterm elections.

Finally, while the discourse around information warfare in America is prominent, we mustn’t forget that this is a truly *global* phenomenon. Allie Funk, a researcher working at the intersection of technology and human rights, explains how the effects of information warfare can be seen across the world. In addition to discussing the challenges and opportunities presented by AI when it comes to protecting human rights, our Q&A with Allie covers the growing surveillance threat to journalists and her advice for anyone working in this field.

When we introduced the “Information Warfare Reporting” class to the Columbia Journalism School curriculum in January 2020, we wondered if there would be enough material to sustain the project beyond the first year. Unfortunately, we need not have worried on that count at least.

1. A Brief History of Information Warfare

By Stuart Anderson-Davis

Stuart Anderson-Davis is a PhD candidate in communications at Columbia University's Graduate School of Journalism. Now based in London, his research explores the history of deception and information warfare in Britain and the United States from the 18th century to the current day. Stuart was a Research Fellow at the Tow Center for Digital Journalism and co-taught the graduate class on Information Warfare Reporting from 2023 to 2025.

Here, Stuart explores several of the key terms associated with information warfare and discusses the history of many tactics and techniques that continue to shape our information environment today, from hoaxing and propaganda publications to front organizations and lawfare against journalists.

Information warfare, an umbrella term for the manipulation of information and information sources, has a long and rich history that remains largely unexplored. Put simply, it's about deception: finding ways to mislead a target audience in order to advance a strategic interest from winning wars and getting elected to making money and embarrassing enemies. While this idea is relatively straightforward, the field is full of confusing and often [contested](#) terminology, including [disagreements](#) over how to define information warfare itself! The jargon is often applied inconsistently — or simply misunderstood — as theories and buzzwords fall in and [out of favor](#) with academics, journalists, and practitioners.

The purpose of this article is to introduce the key terms associated with information warfare and explain the concepts using modern and historical examples from around the world.

TERMINOLOGY: THE BIG THREE

The three core terms of propaganda, misinformation, and disinformation are central to understanding this field, but are often misunderstood or misapplied.



Pope Gregory XV, by Guercino (1622)
https://commons.wikimedia.org/wiki/File:Gregorius_XV_by_Guercino_1622.jpg

Propaganda

The first term is also the oldest. Despite its bad reputation, **propaganda**, as correctly [defined](#), is simply the term for a form of communication (a speech, letter, advertisement, social media post, etc.) that is intended to achieve a desired response from its audience.

The word conjures images of 20th-century totalitarian regimes that dominated mass media via TV, radio, and print to convince, coerce, and cow their people into committing and condoning horrific crimes. However, the word's origins go back much further, to the decision by Pope Gregory XV in 1622 to establish the [Congregation de Propaganda Fide](#) (Sacred Congregation for the Propagation of the Faith). This institution was broadly tasked with promoting and protecting the interests of the Catholic Church, from mobilizing popular support in Europe and advancing its missionary endeavors further afield to countering the so-called "[Black Legend](#)" narrative of Catholic cruelty and sadism that was spread by English and Dutch Protestants throughout this period.

Propaganda and propagandizing should be, strictly speaking, neutral terms,— with no automatic implication that the protagonist is seeking to engineer a *harmful* response (for example, persuading an audience to commit genocide). However, the term's popular association with the Nazi Party and Joseph Goebbels, the [Minister for Public Enlightenment and Propaganda](#), ensures negative connotations that endure to this day.

Misinformation

Misinformation can be [defined](#) as "false information that is shared inadvertently, without meaning to cause harm." These are *accidental* falsehoods, as when North American newspapers in April 1912 initially informed readers that the *Titanic* had not been sunk by an iceberg, but was rather being towed to shore with (per the headline of the [New York Times](#)) "all passengers safe." These reports, a consequence of incomplete telegraph communiques and overzealous journalists, were not known to be false at time of publication, but they nevertheless caused great confusion and anger when the truth emerged.

TACTICS

Disinformation Operations

One reason that disinformation has proved such a popular tool in the arsenal of information warriors is that its impact often lingers long after the falsehoods themselves have been exposed and debunked. For example, in the 1980s the Soviet Union — a regular disseminator of *dezinformatsiya* (as the Russians termed it) throughout its existence — launched [Operation Denver](#), a scheme to spread the false claim that HIV/AIDS was manufactured by the United States military.

The purpose of this operation was to damage the Soviets' great geopolitical rival by sowing confusion and anxiety among Americans, while fueling hostility and suspicion toward the United States from everyone else.

As with other effective disinformation campaigns, Operation Denver was contingent on generating press coverage to amplify and legitimize the lie to target audiences in strategically significant locations, such as India and various African states.

The Soviet scheme proved effective, at least in the short-term, with the [Los Angeles Times](#) revealing in 1987 — in an example of a news organization debunking disinformation too — that the false claims had been published in more than 50 newspapers across the world in the two years since it began. Today, this myth and its [variations](#) still appears on social media and internet message boards with depressing regularity, while its influences could be seen in countless conspiracy theories that proliferated during the COVID-19 pandemic.

As Operation Denver shows, journalists are always found on the front line of information warfare — for better and worse. Courageous, innovative, and resourceful reporting has revealed the existence of many deceptive operations over the past 150 years, exposing the perpetrators and preventing (some) people from falling for the falsehoods. And yet, journalists are also some of the most efficient propagators of disinformation too (unwittingly or otherwise) because their job is to disseminate information to broad and/or specific audiences, which will always make them appealing targets for information warriors of all stripes, from fraudsters to intelligence officers.



Patriot Magazine [India], July 17, 1983, "AIDS May Invade India: Mystery Disease Caused by U.S. Experiments"

https://static01.nytimes.com/images/2017/12/13/us/politics/13dc-disinfo2/mrlin_131179325_4a867223-3bdf-4c56-a5aa-7045df23b618-orig.jpg?quality=90&auto=compress

Hoaxing

The simplest method of manipulating journalists is **hoaxing**: tricking reporters and their outlets into unintentionally publicizing false information. Some of these schemes might be nefarious, as with the fake AIDS story spread to damage the United States during the Cold War. Others might seem more innocent — humorous escapades intended to surprise and delight audiences, albeit by deception.

For example, the [Cottingley Fairies](#) photographs of 1917 — fake images of dancing pixies produced by two young English girls — were shared for decades before they were comprehensively debunked. Indeed, the photographs were convincing enough for Sir Arthur Conan Doyle, creator of the great detective Sherlock Holmes, to publish them (alongside a somewhat qualified verification) in [The Strand Magazine](#) in December 1920.



The Strand Magazine, December 1920,

<https://www.arthur-conan-doyle.com/wiki/File:Strand-1920-12-p462-fairies-photographed.jpg>

Other hoaxes have been motivated by money, as in 1983, when the Sunday Times and Stern magazine were duped into paying millions of pounds for the faked “[Hitler Diaries](#).” Here, the painstaking work of forger [Konrad Kujau](#), a German artist and counterfeiter who produced over 60 handwritten diaries, fooled (at least initially) expert historians and journalists alike.

Of course, these hoaxes seem amateur and antiquated compared to the [deepfakes](#) now proliferating across digital media channels, as A.I. tools enable users to produce bespoke content that seems [more realistic by the day](#). And yet, earlier, much slower to create works of disinformation like the Cottingley Fairies and Hitler Diaries could be just as effective in deceiving audiences at the time they were produced than the content we see today — maybe even more so, given the regular public [warnings about A.I.-generated](#) scams.

Targeting Journalists

Information warfare can include targeting journalists via less subtle or sophisticated methods too. Violence, intimidation, legal harassment (so-called [Lawfare](#)), and the criminalization of journalists and news organizations all suppress the flow of information into the public domain. These tactics are

designed to undermine public confidence in journalists and journalism, while deterring reporters and outlets from covering stories that threaten the interests of those orchestrating the harassment.

This pattern of behavior can be seen across the world — and the situation is getting worse. The [2026 World Press Freedom Index](#) by Reporters Without Borders (RSF) shows press freedom scores at their lowest since the Index began in 2002, while the [number of people](#) living in a country with “good” press freedom has fallen dramatically (from 20 percent in 2002 to 1 percent in 2026) as the legal threats against journalists grow.

Meanwhile, social media has facilitated the harassment of individual journalists. Female reporters have been slandered as “[presstitutes](#)” while many more have been subject to [doxing](#) (“the malicious release of private or identifying information about an individual”) and other forms of cyber-bullying. This combination of online (and sometimes physical) intimidation can be depressingly effective in silencing opposition voices and chilling independent journalism, while exacting a sometimes [devastating](#) impact on individual reporters.

While media intimidation and persecution has traditionally been seen as a non-American trait — one associated with communist regimes and tinpot dictatorships — this [behavior](#) has a long history in the [United States](#), despite the much-vaunted [First Amendment](#) protections afforded to journalists. Indeed, while the Founding Fathers (such as Thomas Jefferson, whose statue stands outside Columbia University’s Journalism School) promoted the narrative that America was a great bastion of press freedom, the same revolutionary leaders who overthrew the British regularly employed journalist intimidation and persecution to advance their interests.



James Rivington (1806), painting by Ezra Ames, New-York Historical Society

One victim was [James Rivington](#), the Loyalist Tory owner and editor of the New-York Gazetteer during the Revolutionary War. Rivington and his “Lying Gazette” were ruthlessly targeted by Patriot propagandists, enduring slander, censorship, boycotts, property destruction, and violence before he finally fled to Britain in 1775. Such methods may be crude, but they are often effective.

Media Capture

If violence and intimidation don’t work, then another option is to seize control of that news outlet — or perhaps even all the news outlets in a particular location. Across the globe, we can see examples of governments and powerful individuals attempting what is known as [media capture](#), a process by which corruption and coercion — usually accompanied by lawfare against journalists or outlets that resist — is used to turn independent news sources into pseudojournalistic vessels for disseminating approved propaganda.

Columbia Journalism School

The most infamous example comes again from Nazi Germany, where Joseph Goebbels' Ministry and the "[Reich Press Chamber](#)" dictated the content of newspapers, films, radio shows, and theater productions to spread self-serving narratives and silence dissenting voices. The Nazis banned news organizations from employing anyone deemed subversive or insufficiently supportive of their regime — including Jewish people. This oppressive model endures to this day, as authoritarian rulers like Russian President [Vladimir Putin](#) and regimes in states like [Iran](#) establish de facto domination of a nation's media ecosystem over decades.

Pink Slime

Media capture on this type of scale is (fortunately) impossible for all but the most powerful individuals and institutions. However, the rise of digital news outlets — combined with the collapse of local newspapers in [America](#) and elsewhere — has created fresh opportunities for anyone seeking to shape public opinion. Today, a wide range of actors from nation states and multinational corporations to political candidates and online provocateurs are [taking over existing news outlets](#), or simply launching their own skewed websites to surreptitiously promote their interests.

Digital outlets that publish "[Pink Slime](#)" — named after the low-quality filling in [cheap meat products](#) — provide a subtler option for those seeking to manipulate audiences by serving them something that [looks like journalism](#) but is more often self-serving propaganda.

Pink slime digital journalism is only the latest iteration of a tactic that has been used by corporate America for over a century. For example, in 1919 the automobile pioneer Henry Ford purchased The Dearborn Independent and transformed the paper into a tool for marketing his cars, but also a vehicle for promoting [antisemitic conspiracy theories](#) to the American people.

Today, corporations are more likely to use their pseudojournalistic sites (which are usually run by PR agencies) to spin positive news about their brands and rebut criticism. These outlets — such as the news site created by [Chevron](#) to reach readers in the oil-rich Permian Basin in West Texas — enable their owners to target audiences in strategically significant locations: a key objective in any information warfare operation.

Sock-Puppets and Astroturfing

Social media is essential for promoting and distributing pink slime journalism. More broadly, platforms like Facebook, X, and TikTok also provide information warriors with the ability to target their content at audiences without needing to trick, coerce, or corrupt journalists into doing it for



The article that signaled the beginning of Henry Ford's seven-year hate campaign against the Jews. (COLLECTIONS OF THE HENRY FORD MUSEUM, GREENFIELD VILLAGE)

The Dearborn Independent, May 22, 1920.

them. These platforms also provide users with anonymity, - should they desire it, or the ability to assume the identity of anyone they please. The use of so-called [Sock-Puppets](#) — a false identity adopted for deceptive purposes — is now [widespread](#) across social media. For example, the exposure of several information warfare operations, including a [Russian scheme to stoke racial tensions in America](#), shows how fake Facebook accounts can be used to sow suspicion, confusion, and outrage.

While social media has supercharged sock-puppetry, this trick can be traced back many centuries further to (at least) the emergence of the printing press. American Revolutionary hero, printing pioneer, and 18th-century polymath Benjamin Franklin frequently misled audiences using pamphlets, articles, and correspondence published under false identities, including one memorable hoax letter written in 1773 (and then published by newspapers) that purported to come from the [King of Prussia](#).

Sock puppet accounts may also be incorporated into a deceptive tactic known as [astroturfing](#), in which support for a campaign or cause is artificially manufactured to make it appear more popular (including with specific groups). The term was apparently coined by former US Senator and Treasury Secretary Lloyd Bentsen in the 1980s. According to the story, Bentsen identified a barrage of letters received by his office (purportedly from concerned Americans) as having been orchestrated by insurance companies, remarking that “a fellow from Texas can tell the difference between grassroots and Astroturf.”

While lawmakers are the most likely target of astroturfing, the tactic can be adopted to engage much broader audiences. For example, a recent investigation identified hundreds of A.I.-generated [pro-Trump avatars](#) on TikTok — apparently one element of an effort to persuade American users to support the president and his administration.



Leopold II, (1865-1909), Private Collection/Carolus
<https://www.britannica.com/biography/Leopold-II-king-of-Belgium>

Front Groups

Franklin and other masters of deception saw the strategic value using false identities that were more likely to interest, engage, and persuade their target audience. Another way to achieve this effect is to create a [front organization](#), an entity that serves as the public face of another individual or group to conceal their involvement.

This tactic was masterminded by King Leopold II, a Belgian monarch who oversaw the brutal exploitation of the Congo in the second half of the 19th century. Leopold’s regime established innocent-sounding societies such as the Committee for the Protection of Interests in Africa and the Committee for Studies of the Upper Congo to mislead politicians, reporters, entrepreneurs, and members of the public into believing that its [appalling abuses](#) in the Congo were actually an example of enlightened evangelical humanitarianism. And it worked — for decades.

Since then, front organizations have been used to advance a wide variety of causes and campaigns, from the CIA promoting American culture and covering up espionage during the [Cold War](#) to multinational corporations like Purdue Pharma concealing aggressive lobbying and avaricious marketing behind the veil of [patient advocacy groups](#).

Conclusion

Of course, in an era of ultra-realistic A.I.-generated content and globally connected digital networks there may be less need for such elaborate (or expensive) tactics. Today's broad range of information warfare operations — from state-led social media schemes to the scams perpetrated by online grifters — rarely require so much cunning or complexity to deceive their target audience. This is a numbers game, too. One company calculated that in 2024 alone the number of deepfake frauds surged by [3,000](#) percent — an increase linked to new online tools that enable perpetrators to cheaply curate personalized videos, images, and audio using content scraped from the internet.

This new frontier of A.I.-powered deception reminds us that information warfare is constantly evolving as its protagonists embrace new technologies and seize on new consumer trends (such as shifting media habits) to promote their interests. Such dynamism makes it even more challenging for those trying to combat the negative effects of information warfare, whether it's teachers promoting media literacy and scrutiny of news sources or journalists, academics, activists, lawyers, and government officials exposing influence operations across the world and targeting those responsible. History tells us that this is a war that will never be won.

2. “Who’s Behind This Website”: Tricks and Tips for Digital Investigations

By Priyanjana Bengani and Jon Keegan

***Priyanjana Bengani** is a Computational Journalism Fellow at the Tow Center for Digital Journalism and a graduate of the Columbia Journalism School’s dual masters program in Journalism and Computer Science. She focuses on using computational techniques to research the digital media landscape. Pri and Jon have both taught in the Information Warfare Reporting class at Columbia, and still routinely share their insights with students.*

***Jon Keegan** is an award-winning tech and investigative data journalist. Jon has taught at Columbia Journalism School for many years and was previously a Senior Research Fellow at the Tow Center for Digital Journalism at Columbia University, researching trust in online news and AI in journalism. Jon has worked at Sherwood News and The Markup, and was at The Wall Street Journal for 18 years, where he ran the interactive graphics team.*

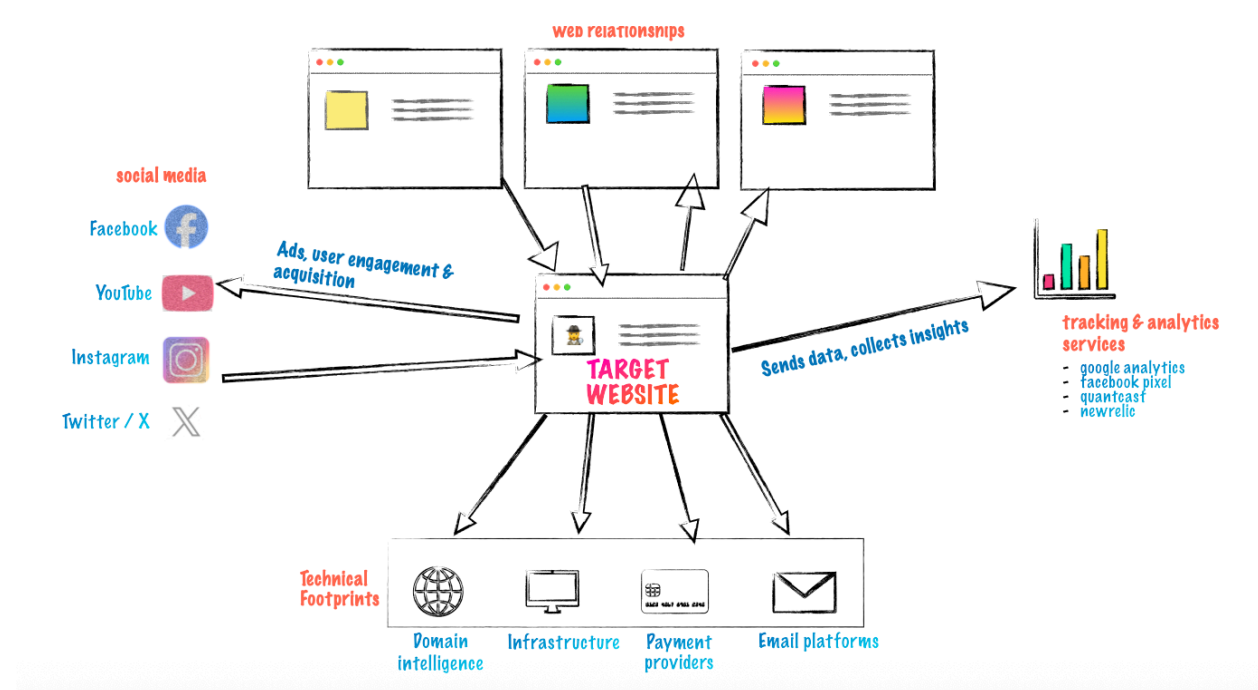
In this resource-packed paper, Jon and Pri share their top tips and tools for investigating online sources, including the growing challenges facing those investigating increasingly opaque platforms, and how to adapt research techniques in a rapidly evolving digital landscape.

Who’s Behind This Website?

We started writing this [guide](#) back in 2022, and the amount of change that has happened since then is hard to comprehend. We wrote this guide because we had observed an alarming rise in websites that were able to mask their creators. Networks of sites full of fraudulent ads and [“pink slime”](#) were seemingly everywhere, with artificial intelligence making the situation worse. We felt the need to gather the various tools and techniques we had acquired and put them all in one place — for ourselves and for other journalists and researchers. Over the past few years, we have presented a version of this guide in several countries at many journalism conferences and to journalism classes.

Today, the same powerful AI tools that have transformed people’s work can also supercharge the creation of vast convoluted networks of anonymous websites to influence, mislead, and amplify propaganda — all while hiding the identities of those behind the operation.

Amid the onslaught of these new threats, the key concepts outlined in this guide will still help a keen-eyed researcher to cut through the fog.



When investigating a website, you can’t simply look at it in isolation. It exists in a larger context, interacting with other sites, platforms, and the infrastructure that underpins the internet. Looking at the entire ecosystem is essential in this process.

The new normal: More opacity, less transparency

A troubling shift away from open platforms has left digital investigators with many pathways for inquiry cut off or severely limited. The town squares of the internet are locked and paywalled, as Twitter became X, and Meta closed off APIs after high-profile privacy and safety failures. Tried and true hacks like [Google search “dorking”](#) and exploring cached versions of search results have stopped working. Many investigative platforms like RiskIQ have been sold to large tech companies like Microsoft, only to be absorbed into other products and shut down.

In a huge blow to researchers everywhere, [Meta shut down CrowdTangle](#) in 2024, removing a powerful tool for monitoring news and information pathways across multiple social media platforms. The company also restricted access to the Meta Content Library to researchers only. That had provided a window into the information that was powering conversations across the world. Now, to get access,

you must declare a research project upfront. The pulse of news across the internet has become much harder to monitor and analyze on an ongoing real-time basis.

WHOIS, the public database for domain registration details, was where you could find the name and address of who's behind a website. By paying an additional fee, registrants are now allowed to hide that information. In 2018, the privacy-preserving GDPR regulation in Europe said that these details are protected personal data and shouldn't be public. This has been a blow to transparency even though you could [argue](#) that cybercriminals and bad actors would have likely provided fake information to begin with.

Large web-hosting platforms like WordPress, GoDaddy, and Squarespace provide good, cheap cover for swarms of websites that can't be exposed through distinct infrastructure, hosting thousands of sites on the same external IP address. Content delivery networks like Cloudflare hide a website's server's actual IP address and only expose a proxy or passthrough IP address to the wider internet. From a cybersecurity perspective, this is incredibly useful — critically, it prevents websites from facing denial-of-service attacks — but it does make it harder to identify how websites are sharing the same IP addresses.

In the wake of Elon Musk's purchase and radical transformation of Twitter into X, many alternative platforms like Mastodon, Bluesky, and Threads have emerged, adding to the challenge of monitoring the flow of information on the internet. Many conversations taking place on public Facebook Groups have now migrated to closed Discord channels and private Telegram chats.

Somebody set this website up! Who? Why? When? How?

Some of the most effective pathways for digital investigations have their roots in the most basic, foundational tenets of journalism — Who? What? When? Why? How?

Who is featured on the website? Are there named authors? Email addresses? Profile pictures?

Always follow the money. Are there payment options — crypto, PayPal, donations, or subscriptions)? If so, who is receiving the money?

Are there signs that the site's owner is trying to stay hidden? Are there bylines of real names for articles, or just generic placeholders? Are authors common across multiple sites, or exclusive to this one?

Why was this website set up? Try to imagine the motive of its creator. What appears to be the intent? To make money through scams or ads (content farms)? To perform some kind of influence operations?

To promote political candidates or social advocacy? To deceive the audience by impersonating another website? To “groom” or “poison” LLMs?

When was this website first published? When was the domain first registered? How long has the site existed in its current form? Was it offline for any significant period of time? Did the ownership change? Be sure to check [historical WHOIS records](#), which can offer a clue. Did the site’s design or content change drastically at any point? Try to create a timeline of the website’s history, and remember that sites are always changing, which can give you important clues of where to keep poking.

How was the website built? What is the tech stack? Where is it hosted? Is it built in WordPress? If so, check the common URL patterns for authors and examine themes and plugins, which can be easily found in the source code. How is the site monetized? Are there affiliate links or advertising? Is the content generated by AI or written by humans? Where does it link to, and who links to it?

While you’re attempting to answer these questions, explore any social media presence the site has. Sometimes, they leak more details — often inadvertently.

Documenting, archiving, monitoring

When conducting complex digital investigations, it is easy to lose track of how you got to a place on the internet. You need to be able to retrace your steps — and have all the receipts — especially in an environment where everything changes all the time.

It’s a good idea to maintain a diary with detailed notes about what you’ve looked at and how you got there. Tools like [Hunchly](#) can be a great way to organize sprawling investigations. Screen recordings through macOS’s built-in QuickTime Player app and screenshots can be useful to keep track of everything you’re doing.

If you have your eye on a particular site, you might want to persistently monitor it for changes. Set up [Klaxon Cloud](#) or [VisualPing](#) to be notified of any changes to a site. It’s also very easy to use [GitHub Actions](#) and [ShotScraper](#) to generate automated screenshots over time.

Things can disappear quickly, or change once a site operator knows they are being scrutinized. Always remember to archive sites consistently (the Wayback Machine browser plugin is great for this), and in some cases, use multiple archival services like [archive.org](#), and [archive.is](#).

For public records or social media posts, take screenshots — some of them might not be archivable. Learn the skills to quickly download online audio and video lest they get taken down. For videos — including those on TikTok, YouTube, and X (Twitter), use the powerful command line tool [yt-dlp](#).

Take screenshots with timestamps so you can monitor changes and gather receipts. The browser plugins [GoFullPage](#) and [ArchiveWeb](#) are great for this. ArchiveWeb also saves all network requests and responses, allowing you to retrospectively analyze the activity in more detail, especially if you're in a rush to get things archived as soon as possible just in case the website disappears.

TIP: Remember to capture the full browser window with the URL field, which strengthens your evidence and helps you retrace your steps.

Techniques are more important than tools

The past few years have led to an explosion of digital investigation tools, especially for collecting OSINT. But the sad truth is that many of those dashboards listing hundreds of powerful tools are subject to “link rot” — tools built as a side project get abandoned as code libraries constantly evolve — or are just scams that overpromise and underdeliver. Some of these tools also use dubious means to collect data, so their output can't necessarily be trusted.

Don't rely *too* much upon someone else's tool for your work, because it could go away tomorrow.

The better approach is to accept that tools (and APIs) will come and go. The key is to learn more about the underlying technology so you can find another way to find your information — or, better yet, build a tool yourself. This is actually one of the most useful ways investigators can use AI.

Instead of asking a chatbot to scrape information from a website you are looking for, learn from AI how scraping works and how to use the foundational scraping tools like [BeautifulSoup](#) or [Playwright](#). Ask your AI chatbot to write the code for a custom scraping tool that you can use, customize, and evolve to fit your own needs. The code will always work, even if your newsroom stops paying the bills for your AI chatbot subscription.

Where possible, use multiple tools for the same question. They can collect data in different ways, so you might find something useful in one tool that another missed.

Protecting yourself online

Each investigation will have a different threat model, so you need to carefully assess the risks to your safety and privacy for each project.

If you don't want to expose your IP address to the target website — potentially leaving a trail back to your location, network, or even employer — use a VPN or Tor. (Note that some VPNs also track your

activity!) Use a browser different to your primary browser in incognito or private mode to ensure any cookies that get dropped during an investigation don't intrude on other browsing activity.

If you don't want to expose your email address to the website, use a different email address when you sign up. Ensure your email client blocks remote content from loading to avoid pixel tracking.

Most email providers, including Gmail, have a way to easily make unique email addresses that will deliver mail to your regular inbox. If your email is janesmith@gmail.com, you can add custom text using the plus symbol. For example, janesmith+sketchysite@gmail.com or janesmith+newslettersignup@gmail.com will both go to the same Gmail inbox. If you start receiving emails about another business to your new email, you know those two sites have shared information.

Some higher-risk investigations may call for the use of a virtual machine such as [UTM](#) or [VMWare](#), to ensure your computer is not vulnerable to the website or tools being used. Beware of opening or downloading PDFs (a well-known vector for malware) and any apps or data of unknown provenance.

Is it ethical? Is it legal?

Just because there is a cool new technique for grabbing information from a website doesn't mean you should go ahead and do it. Always speak to your organization's editors and lawyers before conducting any kind of scraping or probing that could cross ethical or legal red lines. Always make sure your investigation is in the public interest.

Some of the most powerful tools out there are dual use: They can be used to unmask a bad actor, but could also be used to stalk an ex. Paying for a service that deals in ethically dubious practices may cross a line for you or your organization. Be sure to do your due diligence on the tools and platforms you use.

For example, purchasing personal data from a shady data broker might be a convenient shortcut to the info you need, but you could be enabling a greater exploitation of innocent people's privacy.

If you do unmask the owner of a website, consider the unintended consequences. For one, there is still a journalistic question of whether that information should be published. Is it in the public interest? What are the harms that can transpire? Will any innocent party be collateral damage?

Scraping websites for information also can impact the infrastructure of the site you are investigating — and, with bad code, you could even inadvertently take it down. The definition of “[hacking](#)” a website is [squishy](#), and there are serious legal consequences like violating the [Computer Fraud and Abuse Act](#) if you poke the wrong bear.

Journalists should never use a false identity except in the rarest of undercover investigations, and that rule should apply to how you conduct yourself online during the course of your research. Don't use fake credentials or log in as someone else.

Here are some tips for digging into different types of content on websites:

Text

The simplest way to see if a site is linked to others is by seeing how unique its text is.

Check text fragments from articles, **"About us" pages**, and **privacy policies** to see if they are unique to the site or duplicated elsewhere. Use exact string matching on multiple search engines by putting search terms in quotes. These days, many sites use AI-generated policies, so you might get a lot of false positives here.

Scour the site for any names (including bylines), **email addresses**, **phone numbers**, **addresses**, **social media handles**, and **company names**. They all could provide important clues or leads.

When looking for names, phone numbers, or email addresses, use tools like [Epieos](#) and [Have I bBeen Pwned](#) to reverse-lookup emails and phone numbers: Both will show you other services and platforms where the email address or phone number might exist. [Truecaller](#) and [Hiya](#) also serve as reverse phone books. [2Chat's WhatsApp Checker](#) lets you see if a number is on WhatsApp. You can also check Signal, Telegram, and WhatsApp for active phone numbers. Depending on users' privacy settings, you might see a profile picture as well. Note that this isn't foolproof, as users might not allow public lookup of their phone numbers.

If you find **names**, Bellingcat's [Name Variant Search](#) will find possible variations. For **company names**, use [OpenCorporates](#) or [LinkedIn](#) to see whether any employee information is available. OpenCorporates also lets you search by addresses, so you can find who else shares the same office location. Numerous companies listed at the same address can indicate related entities (a win!), a virtual address provider, or a mail-drop address.

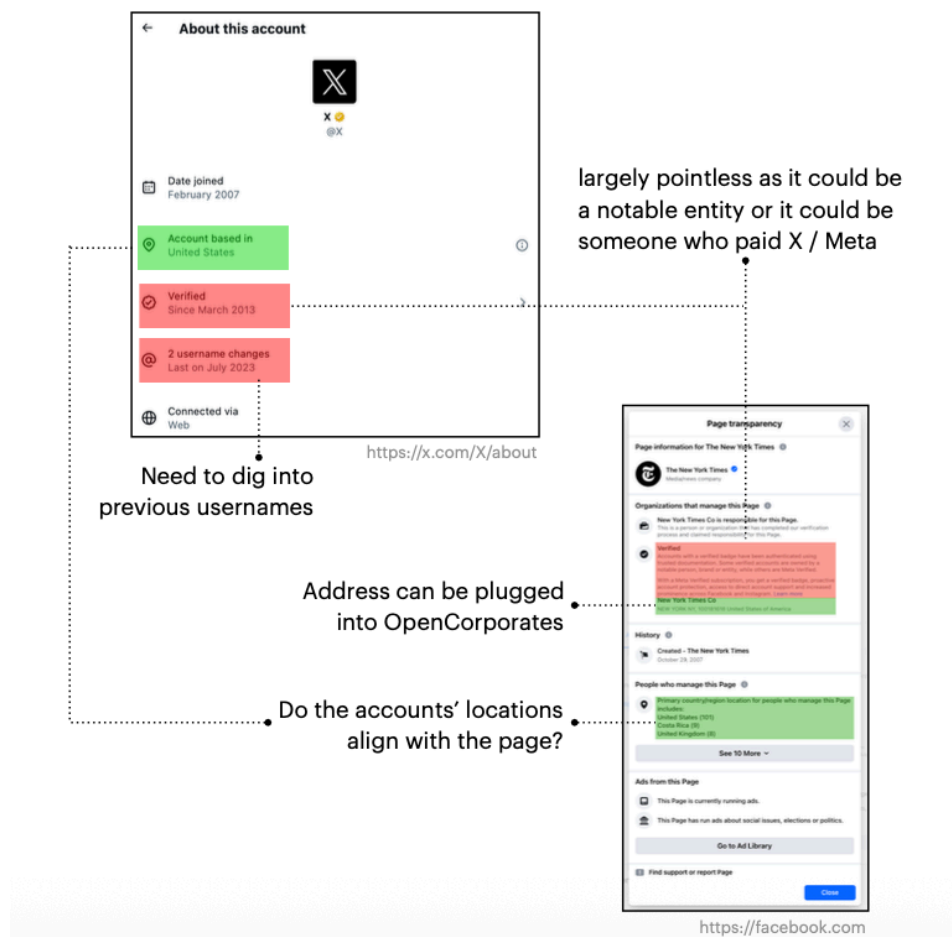
Hacked and leaked datasets can be useful, but if you've not verified the source, you might be vulnerable to malware attacks. Where possible, explore data from obscure sources in a standalone computing environment. [Hacks, Leaks & Revelations](#) by Micah Lee is a valuable resource.

If you find a **Gmail address** and the other tools don't give you a break, open a document in Google Docs and enter the email address in the Share field. If the email address is valid, you should see a profile picture. (Be careful not to accidentally actually share the document.)

If you want to find a LinkedIn profile associated with an email address, compose an email in Outlook and enter the address in the "To" field.

If you find **social media handles**, use [WhatsMyName](#) or the command-line tool [sherlock](#) to scan multiple platforms to see if the same handle appears elsewhere. (You'll still have to confirm that it's the same user and not just the same handle.) You can also see on social media, if those accounts have run ads.

On X and Facebook, you can ascertain the history of an account's page by adding "about" to the link, e.g. [x.com/x/about](https://x.com/X/about). On a Facebook page, you can click on "About" and then Page Transparency to see the page history. This might expose an email address you can then search on OpenCorporates.



Media

Images, photos, and videos all contain data that can contain clues.

Use reverse-image search across multiple platforms like Google, Bing, and Yandex to check whether an image is a stock photo, or if a profile picture appears elsewhere.

For identifying people in photos, you could use facial recognition tools like [PimEyes](#), Yandex Image Search, [Search4Faces](#), [FaceCheck.ID](#), and [Amazon Rekognition](#), but this is definitely a dual-use tool that you should consider carefully.

Look at the website's source to see if there's anything hosted on Amazon's [AWS S3](#). The bucket name can be revealing, and the [bucket might be open](#) if misconfigured.

Use EXIF tools like [EXIF Data](#) to check if any metadata is retained in the images. This can include location, time the photograph was taken, and details of the camera used. Forensics tools like [WeVerify](#) and [InVid](#) can check if media is AI-generated, while [Forensically](#) can tell you whether an original image has been modified or manipulated.

Look at the image names, too: Do they tell you anything about the date the image was taken or the camera it was taken from?

If there are images on any of the social media pages you find, remember to search those too.

Documents

To find documents that might be hosted on your website, use Google “dorking”:

Enter the following into Google's search field: filetype:pdf site:domain_of_interest.com

Also try the filetypes XLS, XLSX, PPT, and DOC. You can use LLMs like ChatGPT and Claude to help construct your Google dork.

write me a google search query to find all pdf documents on US government websites

To find PDF documents on U.S. government websites, use:

`site:.gov filetype:pdf`



To maximize coverage (including subdomains and PDFs that may not be indexed with `filetype:`), try:

`site:.gov (filetype:pdf OR ext:pdf)`



For a specific topic:

`"natural gas" site:.gov filetype:pdf`



To search federal agencies only:

`site:epa.gov filetype:pdf`
`site:energy.gov filetype:pdf`
`site:eia.gov filetype:pdf`
`site:federalregister.gov filetype:pdf`



To find large collections of reports:

`site:.gov filetype:pdf intitle:report`



Or:

`site:.gov filetype:pdf ("annual report" OR "technical report" OR "assessment")`



One limitation: Google will not return *all* PDFs on U.S. government websites because it only shows indexed documents and limits result counts. If your goal is comprehensive discovery, targeted searches by agency (e.g., `site:energy.gov filetype:pdf`) or using agency document repositories often works better than a single global query.

<https://chatgpt.com>

If you find a PDF, open it (ideally in a browser without downloading it, because PDFs can contain malware) and check the document’s metadata for any names or creation timestamps. When dealing with documents of suspicious origin, use [Dangerzone](#) or [Google Drive](#) to prevent accidentally downloading malware.

Donations, Memberships, Subscriptions

If you find any cryptocurrency information on a site, look up the wallet address in search engines to see where else it shows up. Crypto investigation sites like [Etherscan](#) and [Breadcrumbs](#) will show you how much money the wallet has, and how active it is.

Websites might offer a plethora of payment services, from gaming platforms to Alipay, so sometimes it’s worth going through all the steps to see what information you can find out about the payee. (See the [Bellingcat case study](#) “Behind a Secretive Global Network of Non-Consensual Deepfake Pornography.”)

Others

For WordPress websites, you can use the Google author search trick to list any author names in the system. Use a wildcard search following this pattern: “[empirenews.net/author/*](#)”

[WPSscan](#) to see the name of the design theme a WordPress site uses, as well as the names of any authors — which can help you identify sites created in bulk. Pulling a site’s RSS feeds can sometimes show you author names and other information. You can add RSS article links to Google Sheets using [=IMPORTFEED](#).

Archive Services

The [Internet Archive](#) and [Archive.today](#) capture the recent and distant history of websites and social media accounts. In both, you can use a wildcard “*” to find everything captured for a page. This can be especially useful for social media, as a search for “https://x.com/x/*” will find all posts made by that X account.

Internet Archive also has a calendar view that allows you to see the lifecycle of a site: when it first appeared, whether there have been long periods of quiet time, and how active it’s been.

These services don’t back up everything everywhere all the time, so should **not be considered a comprehensive resource**.

For social media, it's typically hard to see how accounts have grown, but you can reconstruct that history using snapshots from archive services.

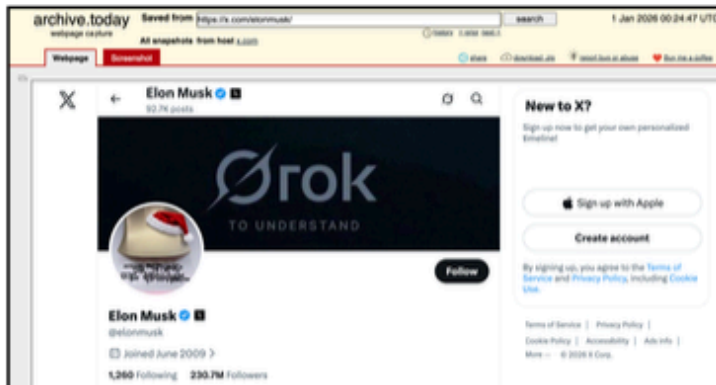
July 2024
190.2m followers



November 2024
203.6m followers



January 2026
230.7m followers



If you see big spikes in follower numbers, it might be worth trying to retrace when or why that happened. When did the account get a big jump? Was it down to a viral post or a boost from an influencer — or, simply, acquiring paid followers? Was the account co-opted?

Infrastructure and networking

When it comes to domains, we need to ask a few questions: Who owns the domain? What other domains do they own? What network, if any, is it a part of?

Consider where this site fits in a larger context of connected sites. Which domains do they link to, and which domains link to it? Where do images and other media load from? Which domains share SSL certificates or favicons? Which other domains share the IP addresses?

Remember: Identifiers are clues — not conclusions.

Adtech

If someone is trying to make money from their site, there's a good chance they are using adtech, which can be examined for clues. Do domains share tracking and adtech identifiers? Which countries' adtech platforms are used? Who are the top advertisers and/or advertising platforms?

Which ad trackers, third-party cookies, and other privacy-encroaching surveillance techniques is the site using? Tools like [Blacklight](#) and [BuiltWith](#) can provide some insight into the motivations behind the site.

Domains

Who owns the domain? What other domains do they own? Look up the WHOIS data for the domain's current and past ownership. GDPR's strict privacy controls have largely obscured this information for newly created domains, but [Whoxy](#) can provide historic domain registration details. Even if details are obscured, you still see when a domain was registered and with whom. Remember that people *can* lie in WHOIS, so it's up to the domain registrar to check. You can search by name, email address, or phone number to find domains registered with the same details. To find other possible related domains, use [dnstwist](#), which gives you domain permutations.

Do other domains share an IP address? Think of an IP address as a phone number for a website. One IP address can host multiple websites, and one website can have multiple IP addresses. Multiple domains using the same IP address can indicate a very strong relationship, but equally sometimes you can get thousands of results — and if you do, abort! This is likely due to CDNs like Cloudflare or hosting services like Squarespace exposing multiple unrelated websites on the same IP address.

Find the current and historic IP addresses of the domain. Find what other domains reside — or have resided — on the same IP address over what time period. Which other domains share the same analytics identifiers? Useful tools for this include [BuiltWith](#), [SecurityTrails](#), [DomainTools](#), [DNSDB Scout](#), and [VirusTotal](#).

Analytics

Identify third-party analytics and tracking libraries used by the website. These include Google Analytics, Facebook Pixel, Quantcast, NewRelic, and Google Tag Manager. Find other domains that share the same identifiers using [BuiltWith](#), [DomainTools' Iris Investigate](#), and [VirusTotal](#).

Note: Google Analytics IDs used to be in the syntax UA-NUMBER-SUFFIX. Related domains shared the same UA-NUMBER, but the SUFFIX was different. Google Analytics 4 changes this such that each website has unique identifiers. Bellingcat's [Wayback Analytics](#) tool looks at the Internet Archive to extract old analytics IDs, which might be helpful in the present and can be used to aid your investigation.

Links

Websites don't exist in isolation. They link to other websites, and other websites link to them. Find who's linking to the website of interest consistently by using a backlink checker like [Ahrefs](#) or [Moz](#).

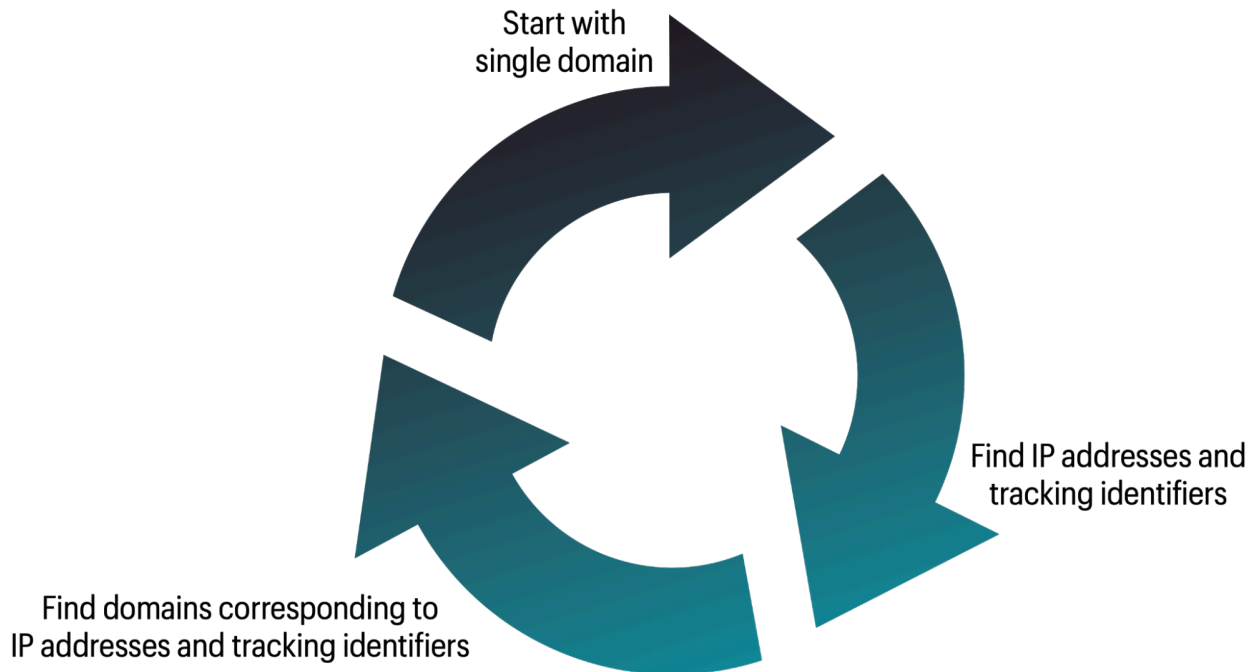
Inbound links may reveal audiences and supporters — especially if you see an inbound link within days of a website launching.

What's the relationship between the sites? Use [Photon](#) or [URLScan.io](#) to gather the outlinks as well as some high-level intel: Who is the site linking to the most? Analyze outbound links, especially those to merch stores, for affiliate links. Who's the affiliate? This is especially useful for investigating health and wellness scams.

Monitoring network requests

It's worth getting familiar with your web browser's developer tools and how modern websites work. Being able to monitor the **network requests** happening behind the scenes is a foundational technique that can be very useful.

Is the site making network calls to adtech providers in other countries? Is the URL for its static files (images, videos) different to the website? Are there any network calls that warrant further investigation? Check the Network tab in developer tools. Who are the top advertisers? Use [FouAnalytics' PageXray](#) to see all the network requests a site makes.



Always remember ...

Everything that goes into a story has to be verified — maybe manually. Just because you found a person’s name doesn’t mean you found the “right” person.

Search obsessively — be it websites, archives, or social media — and set up automated processes if you can (Google Alerts are a good way to do this), because you never know when something will come up.

Combine clues from different services and contexts — there’s no single thing you can do. It’s a combination of things.

Document everything! Things change rapidly, you need receipts, and you can’t rely on your memory!

Additional Resources

Craig Silverman, [Digital Investigations](#) (Substack)

[Digital Digging](#) with Henk van Ess

Jack Creps, [The OSINT Newsletter](#) (Substack)

The [Verification Handbook](#), edited by Craig Silverman

Michael Bazzell, [Open Source Intelligence Techniques](#)

Micah Lee, [Hacks, Leaks, and Revelations: The Art of Analyzing Hacked and Leaked Data](#) (the online version is free!)

3. Q&A: Martin Vassilev on scams, bans, online hustling, and playing cat and mouse with the big tech platforms.

By Michael Keller

Martin Vassilev wasn't that hard to find.

His Skype handle was prominently displayed on his website, 500Views.com — his digital storefront where he sold fake YouTube views.

Martin learned the value of being approachable in one of his past jobs as a customer service representative. It translated well into his current venture. Potential customers weighing the purchase of an ethically and legally dubious service through the internet were comforted knowing that there was a human they could ring up if anything went wrong. They were the ones trying to scam the system, not get fleeced themselves.

Less than 48 hours after Martin took my Skype call — where I explained to him that I was a journalist with the *New York Times* interested in the market for fake views — I was sitting with him in a hotel lobby in Ottawa, Ontario, hearing about his passion for DJing and other money-making schemes, like buying and selling domain names.

“I can deliver an unlimited amount of views to a video,” he told me. “They’ve tried to stop it for so many years, but they can’t stop it. There’s always a way around.”

The article, [The Flourishing Business of Fake YouTube Views](#), was published a couple of months later. Martin and I kept in touch. He still runs his view-selling business, but he’s also changed the focus of his operations as each new wave of technology presents fresh opportunities. He has an algorithmically generated Spotify channel of children’s music; a commercially unsuccessful AI video generation site (it was too expensive to be profitable); and a very successful, above-board SEO company that is now his main business.

For anyone trying to understand why there is fakery online — and *how* these deceptions are produced — seeing the internet through the eyes of someone like Martin is essential. He sees the web as a game, one that only requires wits and hard work to win. He is unbothered by the ethical questions of selling fake metrics and doesn't see much difference between buying views from him or paying Google, Instagram, or others for promotion directly.

Speaking to Martin — and those like him — reminds us that information warriors can be divided into two types: ideologues and grifters. The former wants to use the information space to shape the world after their own fashion. The latter is looking for weaknesses in the attention economy that they can exploit for their own personal gain.

The grifters can be a persistent group, but as Martin's experience shows, they also usually seek the path of least resistance. Some might find more success by going legitimate — although maybe not completely.

[This interview has been edited for length and clarity.]

Q: Maybe you can tell me a bit about how you got started.

Martin Vassilev: This was a crazy journey. It started in 2012. At the beginning I was a DJ, and I was looking at ways to increase the views and likes on my videos. I found [BlackHatWorld](#), which unlocked it all for me.

Q: What is BlackHatWorld?

Martin Vassilev: So, BlackHatWorld is an internet marketing forum and it would provide you with information on ways — not ethically — to make money online, whether it be selling views, selling likes, SEO. ... Anything really to kind of game the system.

Q: What makes BlackHatWorld unethical or of questionable legality?

Martin Vassilev: The fact that people can post on forums, like you can buy Google email addresses, you could buy views, you could buy comments, if I go here it'll tell you how to improve your Google Store rating, Apple rating.

It was also a troubleshooting community. I remember back in the day there would be updates to YouTube's bot detection, and sometimes the views wouldn't work. And I would go to BlackHatWorld

to see if anyone else experienced this issue, or if there was a solution to this, right? To see if there were any other providers that were working.

Q: So going back to those early days, you're a DJ and you're just trying to boost the views on your own videos. How did you do it?

Martin Vassilev: There was a software called U2Views you could download on your computer and it would run in the background and watch other people's videos. The more videos you watch, the more credits you collect, and these credits you can use towards views of your own videos.

And then I was like, okay, so I could probably just use this and sell it on Fiverr. Fiverr was a service where you could sell small services. It was gray in the early days — they allowed a lot of things on there that they wouldn't now.

I was getting so many orders that I paid this guy, who I also found on Fiverr. He was a programmer, because I didn't know anything about programming. I paid to build an app where I could install the software onto multiple computers. I remember I had five laptops running all at once collecting credits. My cost per view was zero, so it was all profit.

Q: And would your software always work?

Martin Vassilev: Well, it depends. Once I started getting lots of orders and I couldn't keep up, I had to find wholesalers on BlackHatWorld.

Q: Can you explain how the wholesale side of this works?

Martin Vassilev: They were websites with APIs that I could connect my website to. So by this time I got banned from Fiverr, and so my developer created 500Views.com and he hooked it up so that any time someone submitted an order, I got notified and I would go and send that person video views by buying them from different wholesalers, which are called "panels." You can buy all sorts of things from the panels now, like Spotify views or App Store reviews, but you need an account and it's harder to set up.

Q: And how are you thinking about — or are you thinking at all at this point — about the ethics of this?

Martin Vassilev: I remember I had no kind of concern about the ethics. No, not at all. There was no concern.

Q: Describe why you're okay with that. Because I think a lot of people would say, "Hey, look, you're manipulating something." And you clearly know these are not traditional marketing techniques. Why do you see it differently?

Martin Vassilev: I mean, I found it more like a game of cat and mouse between me and YouTube, so it was very motivating for me to see how long I could keep this up based on the outcome. The unpredictability. Not knowing if the views were going to work or not. It was a very fun and exciting time.

And it was always fast paced, right? It was overwhelming at times, too. I would get clients who would call in, because at that point there was a phone number — that's one thing that made me distinct from everyone else.

Okay, so before all of this I was working at Dell doing customer service and I learned how to talk on the phone perfectly with Americans. So that experience really helped me out, because I registered a Los Angeles phone number with Skype and I added it on the [500Views] front page and said, "If you have any questions, give me a call." And so that really attracted people and made them think, "This guy's pretty legit." I would get people to call me and I'd have conversations with them and they would buy views and they trusted me a lot more. That really helped, and I was able to talk to them properly on the phone.

Q: The way that you're describing your motivation reminds me of how I see people talk about other disruptive technologies like crypto, where it's kind of giving you an element of freedom, power, money, and fun based purely on your own wits and your own ability to navigate the internet. Is that how you see it?

Martin Vassilev: That was it, Freedom, power, and money. 100 percent correct.

Q: And how long was business good for?

Martin Vassilev: From 2012 to 2019, actually 2018 to 2019, so when your article came out, a couple months later PayPal banned me and I had to reformat the whole structure of the site because I had to integrate with Stripe and I had to make sure that Stripe didn't know it was coming from 500Views. The developer [had] to do a dummy site, so yeah, 2012 to 2018 I was making pretty good income with 500Views. Must have been a million, over a million [U.S.] dollars. Some months I would be making \$20 to \$30k. [For] two years I was making that much.

Then it slowly declined as I stopped putting as much effort into it and started other things. To this day, I'll still make like a thousand bucks or fifteen hundred a month.

Q: Since we first met, you've gone into a lot of different areas. And I always learn something by talking with you because you're always looking at the next thing. I remember a couple of years ago, you sent me that [Wired article](#) about people making music with AI and how it was harming real artists. And I think I said something like, "Oh, that seems kind of dicey and not looking good for musicians." And your response was, "No, this is a great idea. I've just started and I have five different algorithmically and AI-generated bands on Spotify that are making money for me." So maybe describe what you've been doing since then and your different projects.

Martin Vassilev: Well, when the article came out it was a big year, because shortly after I had my first kid and I got banned from Stripe and I wasn't making as much money. So I'm freaking out, and I have to change the way I look at things and focus more on Ottawa SEO, because that was really marketable and I had a good opportunity to gain lots of clients based on ranking at number one for Ottawa SEO.

Q: So Ottawa SEO is your legitimate SEO business?

Martin Vassilev: Yeah, it's registered and everything. And it can be because it's marketable. There's nothing wrong about it. Selling views is a very hard-working business, right? Because you have to find workarounds for everything. You can't just sell ads on Google for it — they don't allow it. It's very difficult.

So I just got into web design and started creating sites. I changed my tagline to SEO and web design service and I've been grinding SEO wise. There's agencies in Ottawa that are big agencies, and I'm ranking better than them on Google. There are four big agencies that have maybe 20 people working for them, and they're still not ranking as high as me.

I'm dominating the SEO field in Ottawa, and it's only me and the AI. And my SEO is working because my clients are staying with me. Their stats are going up.

Q: Are your techniques legitimate? Or are they from BlackHatWorld?

Martin Vassilev: No more black-hat techniques. We now rank our clients using white-hat techniques. No more black-hat! At the end of the day, I'm still doing the middleman job that I used to do with 500Views, finding reliable service providers. I just changed companies.

We are now focusing on building a big network of websites we have full control over and access to. Think of it as a big network hub for Ottawa businesses. We want to own and control 500 websites within the next two years.

Instead of relying solely on OttawaSEO.com to generate business, we will own and operate websites like contractors, plumbing, roofing, HVAC, dental, professional services, and others.

It's the same fundamental skill developed with 500Views: identify demand, find reliable service providers, and connect the two. The difference is that Ottawa SEO Inc. will increasingly own the digital infrastructure that generates that demand.

Each satellite is a legitimate, useful property with original content and real value — not simply a site created to manipulate rankings. Collectively, the network can give multiple independent channels for generating leads, building partnerships, and creating recurring revenue.

Q: How has AI changed what you do in the last three years?

Martin Vassilev: It's significantly changed to my benefit for everything. It's the tool that I've always needed. If it wasn't for AI, I don't know if I would be able to reply to my emails all the time and create SEO reports.

The SEO report would take me so long to do for one client, I would have to type it out. It was impossible. I would need a team, but now with AI, I don't need a team. I can tell it, "Listen, I need a report. Here's the pictures, here's the stats for this client. I need you to provide me with an email report that's professional." And then it does it for me and the client is happy. It's the best tool that has been invented since Google, I think.

Q: Does it help you break the rules, too?

Martin Vassilev: Well, the thing is the tool I use is Replit, and Replit has terms and conditions, and they're very strict on using it. They do have limitations as well, but I'm just using it to create legitimate websites.

I tried to create an app where it fetches all the local businesses, phone numbers, emails, addresses, scrape basically every single location for whatever category I wanted. I tried to do that and it refused. I used it to create an AI video generation site that used Sora. People used it a lot on the free trial, but no one wanted to pay for it.

Q: What's on your horizon?

Martin Vassilev: There's big things on the horizon. The next big thing is apps. Replit just put this update out a few days ago where it connects to your Apple account and you can put it on the App Store so easily. It used to be really hard.

You're going to see a surge in people developing apps in the next couple of years from the people who had the cool ideas that didn't have the money to pay for the coding. I saw, not too long ago, there was a cool app for kids where they just take a picture of something and it tells them what it is using AI. Because kids are curious; they're always asking what stuff is.

Q: Starting around 2016, when the idea of specifically political disinformation became such a big idea in the culture — and now I think it's a pretty common view that people should distrust what they see and read online — with everything that you know and you've done, do you feel like you helped create that?

Martin Vassilev: Maybe somewhat. I was providing an opportunity to people faking their way into being famous. I did help people out. I didn't see it as anything non-ethical. I wasn't hurting anyone, I wasn't making anyone upset. I was probably making Google or YouTube upset, but who cares? I don't care. That's their fault. They should patch their own views system. I was making people happy. So that's really what mattered at the end of the day.

People wanted to increase their views. They were willing to do it. They knew the risks. So when they open up a YouTube account, they read [the] terms and conditions and they know all the risks that are involved. Or maybe they don't, but that's still an opportunity to see if they can kind of win the rat race.

Q: I know that you view yourself as pretty apolitical, but let's say there was some issue that you were very passionate about, and then you saw that someone was on the opposing end and they were dominating the conversation because they were putting out videos, they were getting views, or they were using these tools to really capture the conversation. Has that ever happened to you, or how do you think that you would feel if you were confronted with that situation?

Martin Vassilev: I don't think I would feel anything. I'm really not the type to get caught up in politics emotionally. I don't think I would get affected at all.

Politics — I find that it's all just a game. I've got no kind of say as to what the heck is going on. Just watching the show in excitement and seeing every day it gets more exciting and more unpredictable.

With Trump especially, we've stepped into this reality where we have Trump as the president again and he is completely and utterly just unpredictable.

Q: My last question: What do you see happening in the next five years in this space?

Martin Vassilev: Unpredictable. We don't know what's going to happen in the next six to twelve months. I think a lot of people's jobs are going to get replaced, unfortunately.

There will be new jobs created with AI as well. It'll just be interesting to see how it plays out, and I hope that it turns into the road that everyone is supposed to be on where you have to do something you passionately love, something that excites you, and that's it. That's the way that it should be. You should not live your life any other way. Just use excitement and positivity, and then everything will be synchronous.

100 percent excitement is what you should follow, because we're blessed to have a life like this, and you know it's just an opportunity. And it worries me about the negativity, too. There are things I can't control that are unpredictable. I have two daughters, and there are conflicts around the world that are worrisome. I get worried about things on a bigger scale.

But with AI, I'm not really too worried. I think AI will play itself out. There will be a lot of people that make a lot of money in the next five years. And the capability of AI videos being very realistic — it's going to be very hard to tell if things are real or fake.

4. Infowars in America: Hoaxes, Propaganda, and the War on Rumor

By Professor Andie Tucher

***Andie Tucher** is the H. Gordon Garbedian Professor of Journalism at Columbia University. A prize-winning historian and journalist, she has taught at the J-School since 1998 and has published several acclaimed works on media history, including *Not Exactly Lying: Fake News and Fake Journalism in American History* (2022) and *Froth and Scum: Truth, Beauty, Goodness, and the Ax Murder in America's First Mass Medium* (UNC 1994). Andie served as a speechwriter for the Clinton/Gore 1992 presidential campaign, and has worked in documentary filmmaking and as an associate editor of *Columbia Journalism Review*.*

In this article, Andie explores the intertwined history of information warfare and the American press over the past 250 years, from the “fake news” hoaxing of Benjamin Franklin to the gruesome propaganda disinformation of the world wars. She identifies several key enduring challenges faced by journalists, policymakers, and academics seeking to better understand and address the effects of information warfare on audiences. Perhaps most pertinent for our age of AI deepfakes and algorithmic targeting, Andie focuses on historic precedents for our very current debates about whether rumors and known falsehoods should be exposed to public scrutiny or concealed from view.

Never is the relationship between journalism and power more complicated — nor the incentives to wage infowarfare greater — than in times of war and social turmoil. Never is the job of the news consumer more fraught as infowarriors flood the zone with misinformation, disinformation, propaganda, malice, and mischief designed to support their own side and boggle the other. In this context, people determine for themselves what they *want* and *expect* to be true.

Something similar could be said about the first 200 years of American journalism as a whole. Beginning with the very first American newspaper in 1690, many publications included a voluptuous variety of nonfiction, fiction, and quasi-fiction in their columns. And their readers were rarely surprised or bothered to encounter items that might not be factual; they understood it was up to themselves to decide what they *wanted* and *expected* to be true.

In the last century or so, however, ideas about how journalism should work have undergone a critical change. Among the catalysts were the enormous stakes of the global battle against totalitarianism; evolving understandings about the role of journalism in a democracy; the vast reach of the mass media and the recurrent disruptions by new technologies; the apparent ubiquity of enemy propaganda; the lingering distaste for how infowarfare had played out in previous global conflicts; and the rising public distrust of government, the press, and other powerful institutions, to name but a few. Yet, as Americans came to expect that most of what they read in a newspaper was verified, factual, and accurate, leaders and the press alike faced new conundrums: How should truth look in wartime? What distinguishes truth from misinformation, fake news, and lies? How could they tell the truth about lies: to persuade people *not* to believe the false things they *wanted* and *expected* to be true?

To be sure, Americans had long valued and embraced journalism as an essential tool for the working of democracy, critical for informing citizens about public questions. Through the end of the nineteenth century, newspapers were Americans' primary source for news and information, serving up political intelligence, partisan arguments, and important facts about everything from cholera outbreaks and murders to steamboat schedules, local marriages, and the price of corn. The U.S. fondness for smelly columns of newsprint was something of an international joke: European visitors like the author [Mrs. Trollope](#) wrote home snickering at how many newspapers Americans read and how many Americans read newspapers.

This was an era when other kinds of reading material could be scarce, and fact-based *reporting* lay beyond the reach (or even the imagination) of many smalltown editors — some of whom resorted to labeling dubious items with the irrefutable headline “Important if True.” Newspapers also sprinkled their columns with jokes, tall tales, hoaxes and humbugs, rumors, poetry, fiction, humorous sketches in regional dialect, ads for miraculous cure-alls, and unsourced yarns of wonderment or tragedy, all mixed indiscriminately with the news of the cholera and the corn. Readers understood that any encounter with a newspaper required — or allowed — them to apply a skeptical eye and decide for themselves what to believe.

Infowarfare, the manipulation of information for strategic purposes, blended well into that journalistic landscape. During the era of the American Revolution, Patriot newspapers played an essential role in boosting the morale of the citizenry, while pro-British editors often endured harassment and boycotts. In 1770, Patriot newspapermen made sure readers understood the full heinousness of the British actions in the Boston “[Massacre](#)” — which was actually more like a riot in which, as the British captain later [described](#) it, club-wielding Patriots using “the most cruel and horrid threats” taunted and harassed the edgy Redcoats into opening fire.

Hoaxing was a key part of the conflict, too. For example, in 1782, just as the peace talks with the British were opening, the sage Benjamin Franklin himself faked up an authentic-looking “[Supplement](#)” to the *Independent Chronicle* that detailed grotesque atrocities committed on American citizens by the



FIGURE 1. Franklin's hoax, *Supplement to the Boston Independent Chronicle*, first edition, printed at the press at Passy, April 1782. American Philosophical Society. Reproduced with permission.

Redcoats' Seneca allies. His hope, he said, was to make the British ashamed of themselves at the talks, but in this case the fake was so lurid that the British politician and writer Horace Walpole, for one, guessed the real author.

Ninety years later, the brutalities and disruptions of the American Civil War — the first full-scale war to be covered by a truly mass media — inspired a cornucopia of hoaxes, shams, and frauds, driven by motives ranging from expedience to politics to personal profit. For example, battlefield photographers sold [images](#) of sprawled corpses at Gettysburg, the most famous battle of the conflict. Some of them were described as showing the bodies of “calm and resigned” Union men who “had a smile on their faces” even in death, and others as Rebel soldiers who “paid with life the price of their treason.” They were the same bodies photographed from different angles.



Gettysburg, July, 1863. Photographed by Timothy H. O'Sullivan. Prints and Photographs Division, [Library of Congress](#). Reproduction number: LC-B8184-7964-A

Gettysburg, July, 1863. Photographed by Timothy H. O'Sullivan. Prints and Photographs Division, [Library of Congress](#). Reproduction number: LC-B8171-0234

Other hoaxes sought to stoke tensions yet further. During the election of 1864, an anonymous mass-circulated [pamphlet](#) made the incendiary argument that the offspring of racially mixed marriages were “much superior, mentally, physically, and morally, to those pure or unmixed.” This work was produced not by the abolitionist activist who was purported to have authored it, but by two

mischief-making journalists on the Democratic *New York World* who were eager to stir up anti-abolitionist passions.

A few decades later, during the Spanish American War, the brutally competitive “yellow” papers wrangled fiercely with each other for scoops from the front line, the more sensational and startling the better. William Randolph Hearst’s *New York Journal* reveled in purple provocations about lustful Spanish grandees strip-searching innocent Cuban maidens — a story that had the additional advantage of justifying the publication of a large, realistic-looking engraved [illustration](#) of a woman who was both innocent and naked. (The maiden, a messenger for the rebels, was not actually searched by male grandees in public, but by matrons in private.)



New York Journal, 1898, https://commons.wikimedia.org/wiki/File:Spaniards_search_women_1898.jpg

Meanwhile, audiences thrilled to Thomas Edison’s newest technological innovation, flocking to movie theaters to view images of combat scenes that actually moved, just as in real life! The audiences weren’t told that the hat-waving, gun-toting onscreen figures labeled as [“U.S. Infantry supported by Rough Riders at El Caney”](#) in Cuba were actually rakishly outfitted New Jersey National Guard members in the woods near Edison’s studio in West Orange. Filmmakers suppressed the dirty secret: It was too difficult and too dangerous to maneuver bulky movie cameras on the real field of battle.

It was in the early 20th century, however, that public awareness of infowarfare really came into its own.

The propaganda and hype surrounding World War I became infamous as leaders on all sides sought to explain and justify an increasingly inexplicable global conflagration to their publics. Allies pictured the Germans as subhuman savages who raped nuns, chopped off babies’ hands, and merrily cooked down

the corpses of their own soldiers to render their fat into soap or munitions grease.

Real, exaggerated, and fabricated German atrocities during the so-called “Rape of Belgium” in 1915 were the foundations of the public villainization promoted by Allied propagandists. Lord Bryce, a former ambassador to the United States, lent his name to a widely circulated British government [report](#) based on hundreds of depositions taken from Belgian refugees and others detailing the crimes committed there.

Many of the depositions — the originals of which mysteriously vanished after the war — were anonymous or based on hearsay, while few (if any) were taken under oath. But that didn’t stop U.S. newspapers from eagerly spreading the word with screaming headlines like “BRYCE REPORT SHOWS MURDER LUST AND LOOT. British Government Commission Investigating Alleged Atrocities in Belgium Convinced Stories are True.”



Oregon Daily Journal (Portland), May 12, 1915.

The Second World War that broke out only two decades later brought about a radical change. Chastened by the mistakes and excesses of WWI, the White House took a different approach against the Axis forces. It embraced (if it didn’t always attain) what Archibald MacLeish, the head of the War Department Office of Facts and Figures, pointedly called a “strategy of truth.” According to MacLeish’s 1942 speech to the Associated Press, this approach was intended to counter “the frauds and the deceits” of the enemy with the “simple and clarifying truths by which a nation such as ours must guide itself.”

This different approach required different tactics to inform the public about the progress of the war. Among those were a pair of efforts — one directed by the White House, the other led by a loose coalition of civilians — each of which identified *rumor* as the same particularly lethal menace to national security.

“Breeding sometimes in the stinkholes of enemy propaganda,” [Life](#) magazine reported in October 1942, “sometimes in the muddled minds of gossips and show-offs, it spreads through a community with the rapidity of measles. It damages public morale as effectively as infectious disease damages public physique. Its most dangerous carriers are innocent folk who love to tell a tall tale.”

In 1944, the social psychologist Robert H. Knapp [wrote that](#), like mythology or folklore, rumors “gather impetus from the emotional gratifications which they afford.” In other words: rumors told people the things they hoped and wished were true.

So was it possible to tell the truth about lies? And what tactics should be used in pursuit of truth? Here, the two anti-rumor efforts differed radically over whether the better weapon was science or sunlight — whether the stronger strategy was education or exposure.

The White House's Office of War Information (OWI), which was consolidated in June 1942 from various alphabet-soup agencies devoted to informing the public, focused on data collection and analysis. Its leaders thought that the best way to stem the flood of harmful rumors loosed by the Axis powers was to educate Americans on how to recognize them. To do this, the OWI gathered and studied rumors in the wild to understand how and why they worked.

The OWI recruited educators and students at dozens of universities to collect rumors, complaints, and comments about the course of the war from teachers, barbers, grocers, dentists, community leaders, and others in a position to hear (or overhear) such materials. Their job was to pass them on to the appropriate officials for analysis.

Wary that repeating rumors even to debunk them would only entrench them more firmly in people's minds, the OWI did not make the rumors themselves public. Instead the rumors were used as guidance for determining where corrective, fact-based information campaigns were most needed. And with its insistence on maintaining tight control over all public information about the war, the OWI's leaders eventually decided not to cooperate with academics, who, they felt, could not be trusted to follow the government line.

Sidelined from the official government operation, some scholars and other civilians keen to help the war effort or intrigued by the opportunity for research went rogue. In early spring of 1942, planning for the first so-called "Rumor Clinic" began under the guidance of (among others) the Harvard social psychologist Gordon W. Allport. He was convinced that the best way to defang rumors was to publicly, specifically, and aggressively expose and correct them with facts vetted by experts. He centered his project on newspapers and public engagement.

The campaign against rumor quickly caught on and dozens of other communities soon set up "clinics" of their own. All of them invited people to submit any rumors they heard to a designated local agency — such as the committee on public safety, the chamber of commerce, a newspaper — for review by "responsible" people. Submitters were required to include their names and addresses, but neither those nor any identifying personal details about their subjects were printed. In some places, volunteer "morale wardens" were also assigned to keep their ears open in public and report what they heard. Once a week, the local paper would select a few to publish and authoritatively refute in a column under the bold headline "Rumor Clinic." This one, from the *Atlanta Journal* of 12 November 1942, was typical.

RUMOR CLINIC

The Truth About Knitting for Troops; Outlook as to Gas Supply for Homes

RUMOR: "Knitted articles being made for the Red Cross are a useless expenditure of time. None of the men in the last war used them. One ex-soldier says the only knitted garment he ever saw was being used to wash off a horse with."

FACT: General James H. Reeves, executive director, Atlanta Chapter, American Red Cross, says: "The above is a canard that originated in the first World War and is still going the rounds. As one who commanded a regiment of infantry (some 3,700 men) in active operations in France, I can personally testify that all the knitted goods furnished to the men by the Red Cross were gratefully received, constantly used and highly prized by the men."

"On January 27, 1942, Mr. R. R. Guthrie, chief of textiles, clothing and leather goods branch, stated, 'The War Production Board does want women to knit sweaters where absolutely needed by the armed forces and where the commanding officers ask for the supplies.' This is a system we have set up with the Red Cross. . . . In this way every sweater will serve a good purpose and there will be no waste of material, to say nothing of the labor of some patriotic women."

"The Atlanta Chapter has received numerous postcards and letters from men in the armed forces, in many places, expressing thanks . . . for knitted goods received and testifying to the need for them."

Atlanta Journal, 12 November 1942

Rumors of all sorts were caught in the clinics' webs. Many had clearly been created to sow division and discontent by accusing "outsiders" of receiving special treatment or exhibiting unpatriotic behavior. False rumors included:

- A network of "Eleanor Clubs," named for First Lady Eleanor Roosevelt, was reportedly encouraging Black female domestic workers across the South to walk off the job.
- Jews reportedly evading the draft with the help of Jewish doctors.
- Six thousand Black soldiers dying when their transport ship sank through "gross carelessness or unnecessary exposure."

- Married white men being drafted into the armed forces, while single Black men were not yet being called.
- Women without skills or training being paid the unprecedented sum of \$40 a week to work in defense plants.
- Guns made with substandard steel blowing up in “the faces of our boys.”
- Warnings that buyers of war bonds would never recover their investment.
- Claims that the Red Cross was selling blood that had been donated by volunteers.

While many rumors bore the hallmarks of Axis propagandists, others could just as plausibly have originated in the homegrown racist and antisemitic tropes entrenched in America long before WW2.

Even rumors that now seem impossible or silly were treated as potential threats to morale. There was the one about 15,000 soldiers sent home from Alaska with frozen brains. The yarn about the young munitions worker with gunpowder residue in her hair who ducked into a salon for a perm and had her head explode. And the claim that two of the eight Nazi saboteurs who landed on the East Coast by U-boat were spared execution because they were Democrats. (The *News* of Paterson, N.J., did dub that story one of the wackiest it had seen.) Whether rumors originated from a gossipy neighbor or had been maliciously crafted by an enemy agent, they could be bad for morale, and all were showily debunked.

Besides their opposition to rumor, the government and civilian projects had something else in common. Although their different strategies, goals, and products don’t make for easy comparisons — and it’s impossible to trace how many minds might have been changed by either effort — the disappointing conclusion is that neither science nor sunlight could be judged as particularly successful in combating rumor.

One major problem, as leaders of both projects would later acknowledge, was that people weren’t exactly sure what actually constituted a rumor. In fact, some struggled to find juicy ones to report. The field representatives who submitted regular reports to the OWI — many of which are now held [in digitized form](#) by the Library of Congress — frequently explained apologetically that they didn’t have any rumors to send in.

“No rumors, related in any way to the war effort, were heard from August 3 to August 15, 1942,” [wrote](#) the representative from Arkansas. “There seems to be a sudden lull in rumors. I have heard only one this week,” [confessed](#) the OWI’s man in Alabama around the same time.

One Florida rep struggled to make a virtue of his failure, writing that one of his informants, [reported that](#) “contrary to hearing rumors, he has been both amazed and delighted by their almost non-existence. He is a man of keen perception and is so widely known that he surely would encounter rumor material in his official contacts and travelling by bus and train, if it had any volume of spread.”

Both the official and unofficial antirumor campaigns had a [lettre de cachet](#) vibe about them, with many of the so-called rumors sounding less like enemy propaganda than personal complaints by people

hungry for someone to listen to their grievances. The landlord in Kentucky who [told](#) the OWI man, “I don’t like to have Army officers in my house ... they give too many drunken parties” might have been embroiled in a Nazi plot to defame military men as untrustworthy and boozy louts. Or he might simply have been tired of cleaning up after rambunctious young men and welcomed an opportunity to share with a listener his grumbles about vomit on the walls.

Many of the Rumor Clinic columns, too, reflected frustrations about *other* people’s behavior: They’re cheating, they’re wasteful, they are finagling with tires or gasoline or tin cans or sugar. It’s of course understandable that the stresses and anxieties of wartime contributed to a pervasive sense of suspicion. But it’s also not impossible that at least some readers found a sense of purpose in the tacit invitation to spy on their neighbors, or a feeling of vindication from reading the anonymous denunciations in the weekly columns. Despite the earnest efforts of the rumor warriors, some Americans did not want to be told that the things they *wanted* and *expected* to be true ... were not.

By the end of the war, the Rumor Clinics had faded away. The OWI, which continued to insist that publishing rumors would only strengthen them, was making concerted efforts to strangle the clinics in red tape even as public interest dwindled, fewer rumors were submitted, and newspaper editors found the columns less compelling.

But even so, the World War II rumor projects — which numbered among the first serious institutional attempts to challenge the falsehoods of infowarfare with targeted, verified, and authoritative counterarguments — deserve some credit as precursors to the fact-checkers and investigative reporters of today who insist on the difference between truth and lies.

It’s gotten no easier. The media landscape, it seems, is going backwards, resembling more and more the newspaper of old with its chaotic columns full of jokes, hoaxes, fiction, yarns, and, yes, rumors, from which readers were invited to pick and choose for themselves what they would accept as true. In fact, today’s landscape is even more challenging because infowarfare can spread digitally even faster and farther, outracing any attempts to swat it down while offering like-minded consumers the seductive illusion that they are “doing their own research” and “making up their own minds.”

The efforts by World War II rumor projects to establish themselves as credible and authoritative voices for news in a time of crisis were laudable, if ultimately over-optimistic. Whether their tactic was sunlight or science, these projects offered what seemed the only possible counter to infowarfare: information vetted and verified by people in a position to know what they’re talking about. Information that might succeed in persuading people *not* to believe the false things that they *wanted* and *expected* to be true.

5. Q&A: Researcher Danielle Tomson discusses her experiences studying MAGA influencers, pre-bunking social media falsehoods, and the difference between rumors and disinformation.

By Emma Goldhaber

Danielle Lee Tomson is a writer, scholar, and strategist who has written extensively about information warfare, including analysis of political influencers, populism, propaganda, and election misinformation. Now working at the Center for an Informed Public at the University of Washington. Danielle has a PhD in communications from Columbia University's Graduate School of Journalism, where her many achievements included TAing for the Information Warfare class for several years!

In this interview, Danielle discusses her work examining conservative social media influencers in America, including her time alongside key figures like Steve Bannon, Jack Posobiec, and Laura Loomer, which is the subject of her forthcoming book: [*Under the Influence: What's Real When America Feels Fake?*](#) [to be published in February 2027]. Danielle also looks ahead to the 2026 midterm elections and offers guidance for anyone studying the darker spaces of the internet.

[This interview has been edited for length and clarity.]

Q: How would you describe to people what you do?

Danielle Tomson: At the [Center for an Informed Public](#), I'm a research manager overseeing two different groups. One is leading our [election rumor research](#). This is a rapid research team that discovers, analyzes, and then communicates and translates knowledge about emerging rumors related to election integrity, processes, and procedures. It's funny. We made a [bingo card](#) recently drawing on tropes data coded by members of the team: It was based on over 30,000,000 different tweets. They identified 150-some recurring tropes, and they just keep coming up in the past five years, to the point that it's almost predictable. Though discovery and analysis of new rumors is important, just as critical is explaining to the public the sort of underlying deep stories, narratives, tactics, strategies, and tropes that we keep seeing, and that we will see.

Our interest now is definitely turning towards improving institutional and academic communication for the public generally. I think there's a lot of experimental and exciting research questions about how you can make expert knowledge — particularly about breaking news events — more accessible to different public stakeholders, whether those are journalists or election officials or increasingly content creators themselves who are in different domains. My [colleagues](#) have [published](#) some great work to this effect, and we produce white papers about [our methods](#) as well.

Q: Is that something you're seeing from institutions more broadly?

Danielle Tomson: For years and years, public-serving institutions have faced so many cuts to their basic functions, to say nothing of their efforts to communicate with the public. And I think, as liberal democracies are under attack, we really need to think about the common sense and worldview underneath *why* these institutions exist; how they need to be improved, and what they're doing now that's *essential*. And doing that in a way that isn't just advertising, but a real communication effort with the public.

I talk a lot about this on my Substack, [Failure to Communicate](#). I'm really obsessed with how we communicate with each other more effectively, especially things that we might take for granted, like liberal democracy or expertise or parts of the administrative state [such as] public health. All of these things that I think people always wanted to improve, but don't sometimes have [the resources]. ... I've lived in different countries and in different places where those state apparatuses are maybe not as strong, or may be corrupt, or don't exist. I think you have to validate *why* they should exist sometimes and remind yourself with every generation.

Q: Before you started at the CIP, you undertook a PhD in communications at Columbia University. How did that experience inform your perspective?

Danielle Tomson: A lot of [my work] is informed by my doctoral research, which I turned into a book called [Under the Influence: What's Real When America Feels Fake?](#) The [dissertation] was an ethnographic study I conducted that was based off a chance meeting with Steve Bannon back in 2017, where I was seated next to conservative media influencer and journalist [Raheem Kassam](#), who was the founding editor of Breitbart UK. That whole thing spawned this series of offline relationships with really online personalities, including Jack Posobiec and Laura Loomer.

This was really early on in MAGA, when I think that there was a huge amount of novelty [in] these content creators and vocal political actors online that were saying words and concepts and stories outside the pale of "respectable" politics. I think today we're like, "Yeah, this is just the water we swim in." But ten years ago, it was really novel.

Q: How did you cultivate those sources and get them to talk to you?

Danielle Tomson: I think part of it was because I think positionality is really important. I never thought of them as sources so much as *subjects*. They were part of an ethnographic research study. Mind you, I didn't have much in the way of a public persona then. I was sort of a no-name graduate student for the most part, who was interested in civic technology and online communication.

And I was also wondering why my dad voted for Trump in 2016. I come from a rural western Pennsylvania family who really resonated with that Trump "forgotten man" tale of people not talking to us in a way that they resonated with. I grew up very close to Butler, Pennsylvania, where in July of 2024, there was a [Trump assassination attempt](#). And the firefighter who [was killed](#) often sold 50/50 raffle tickets at my family's dirt car track.

So I came from a family and a community that wasn't like cosmopolitan, leftwing elites. I think by virtue of that, I understood the story that those subjects [like Bannon or Kassam] were telling, even when in some ways some of them were more cosmopolitan than me by birth, growing up in cities or places that were much more urban than me.

When I spoke to them, it was very important that I got in through a community of other folks who were conservative. It wasn't a cold reach out. It was through community connections. And I think that's something we don't talk about enough to graduate students: that I think research is a deeply personal enterprise. So many people study the things that are closest to their soul, not only like their social proximity (that too), but because they're trying to figure out something about how the world works that deeply confuses them. Because why else would you spend five to seven years of your life [doing this] when you could be making a lot more money or having a lot more fun?

For me, that was exactly it. I was deeply confused and concerned and curious about this. And I didn't come at them in an adversarial way. I wasn't asking them: "Why are you a sexist or a racist?" That's not a good question to ask someone if you want revealing answers. I wanted to know their motivation for doing this work, their stories, how they did their work, and who they worked with. I got interested in them as people in a larger ecosystem with different incentives that inform that power.

At the time, a lot of researchers didn't have access to those people. But they had access to what they were saying online. So there was a lot of disinformation research: this digital media research that relied on pulling tweets from the Twitter API or studying rhetoric on different platforms. ... All of that is really, really important knowledge. But, ironically, I had this personal access to some of these content creators who [were] on every list of "disinformers," whether that was in the Trump elections or January 6, for instance, as influential "[newsfluencers](#)."

I got really interested in this question that regular people were asking me: “Are these guys for real, or are they just fucking with us?” Because they were saying these things that sometimes seem so grandiose, or so beyond the pale, or so racist, or so pugilistic, that it felt like they were living in a different world or something. And I got really interested in, not just that phenomenon, but that feeling of, “Is this for real?”

Q: What did you find?

Danielle Tomson: There’s this rhetorical tool I use in the book called the “[Authenticity Gap](#),” which is this experience of when the lived story — the stories you were told about how the world works, about capitalism, about success, about climate change, about universities or government. ... When they don’t align with your *lived* experience of those things, it creates almost like this epistemic break.

And that’s what I call the Authenticity Gap. And what these guys did — whether it’s Bannon or Posobiec or Kassam or Loomer or whoever — they went into that gap and they said, “Yeah, you’re right. Those stories, that’s not how the world works anymore.” And what they try to do is *renarrate* reality. And this isn’t something that comes from polls or focus groups. This is a very creative and performative project. And so to answer that question, are these guys for real? My answer is yes, they’re performing sincerely.

Q: Can you talk more about what that performance looks like?

Danielle Tomson: There is a part to the technological, rhetorical, political, and social incentives of being online and expressing yourself. You have to do it to get attention and get your word across. But also on a deeper level, almost like a spiritual level, you have to be the change you wish to see in the world. You have to fake it till you make it, which was really the zeitgeist of the 2010s. I invoke [Adam Neumann](#) early on in the book. With WeWork [the company he cofounded], it’s like he thought that creating this coworking space was going to change the world. And, at the time, some of us kind of believed it. This is the 21st-century way of doing things. We’re going to model this new way and it sounds absolutely bonkers, but you have the balls to build it.

And I think that can feel crazy to people sometimes. That performativity allows you to create something into existence. And a lot of people don’t want that. They don’t want the world that those folks want: that the nationalist-populist right wanted to create. But some people *did*, because it was better than what they thought they had. And it was speaking to them in the languages and styles that they understood — like tabloid culture, pro wrestling, or sports — or all of these things that are accessible to a lot of different sectors of Americans who maybe aren’t news junkies.

That's what I'm really interested in. At the end of the book, not to spoil it, but, they achieve power! Trump gets power. And the stories that they told do not necessarily align with [the] lived experiences that people expected. So you have that Authenticity Gap again, and there's a big opportunity to come in and create something new. But that's going to require more than just policy and research. It's going to require something really creative and imaginative that is *mostly* rooted in the real, but some of it can't be rooted in reality because some of it has to imagine tomorrow, and tomorrow doesn't exist yet.

Q: Speaking of imagining tomorrow, some of your work involves “pre-bunking” rumors related to US elections. Can you talk about how that works?

Danielle Tomson: This was something we did with our [CIP] election rumor research team in the summer of 2024, working with journalists to get the public aware of anticipated kinds of misleading rumors that can be taken advantage of by a variety of actors. We keep in mind some rumors may be true, some may be false, most are something in between. Some are indeed products of disinformation campaigns. We know there are certain kinds of narratives or tropes that are gonna get out there. We need to get the word out that this is something that people should expect to see — but these rumors aren't conclusive!

[Studies have shown that pre-bunking](#) can increase confidence and reduce the belief of fraud in elections. And I think we at the CIP have [the] capacity to help with pre-bunking and support journalists' efforts to alert [the public] that some people are going to, for example, falsely allege that mass numbers of noncitizens voting will happen, or that there will be glitches in voting machines, implying some kind of nefarious intent.

Rumors are a reaction to moments of high uncertainty in domains that most people don't know a lot about, such as election administration. While some rumors turn out to be true, many are exploited in one of the “five moves” of [misleading election rumors we've identified](#). Rarely, rumors use 100 percent false “evidence,” but most of the time they may misinterpret real evidence like photos or videos, omit remedies to real problems, exaggerate the impact of an issue, or falsely attribute intent to actors involved.

We've seen that the president has this ongoing narrative that elections are insecure or under threat, or that folks who shouldn't be voting are voting, or that the 2020 election was stolen. We have so much data researching this through the years that we know that there will be certain narratives at this point that are either misleading or false.

Because we monitor these platforms and the narratives and the stories that are being told about them, we are able to anticipate and share knowledge of these dynamics.

Q: When you were first talking about how you describe what you do, you used the term “rumor.” Can you talk about the use of “rumor” versus “disinformation?”

Danielle Tomson: I think if you approach everything you hear about online as “disinformation,” you might be misinforming yourself. Because a lot of people go online to try to make sense of the world in moments of uncertainty. And moments of uncertainty are highly vulnerable moments — whether it’s an election, a natural disaster, an assassination attempt — where you don’t have a lot of verified information. And in that uncertainty, in order to calm our epistemic nerves, we want to know what’s happening. That’s why we spread rumors. That’s why we share information. I think that’s a really human urge.

I’m building on the [work](#) of my colleagues Kate Starbird and Emma Spiro, and a decade of research into “rumor dynamics,” which is what they were calling it before disinformation was even a widely used term. They were studying crisis informatics. How are people making sense of things in a crisis moment? People will earnestly and honestly share information that can later on turn out to be wrong. It’s not necessarily malicious.

Disinformation is the *intentional* spread of false or misleading information to serve some sort of purpose. Not all of the stuff that you see on the internet is that. It’s really important to understand the distinctions of these information dynamics. Lord knows there are verifiable disinformation campaigns happening, particularly during election season. It’s a more empirically honest thing in a moment of uncertainty to call something a rumor, unless you are sure that it’s part of a disinformation campaign.

Q: What kind of impact does this research have on you?

Danielle Tomson: Studying the internet includes the scary stuff, right? The propaganda, the hate, the mis- and disinformation campaigns, the crises. You’re studying things like war and violence and hate speech. These are really ugly places, but the internet also has a lot of beautiful and funny places. I think, most of the time, that’s where most people are spending their time, because most people are not, quote unquote, disinformation researchers, looking intentionally at the worst shit on the internet all the time.

You have to remind yourself that a lot of times people make sense of the world we live in through distinct cultural spaces with their own rhetorics, aesthetics, and shibboleths. And some cultures give them comfort, whether that’s sports metaphors, or religious ones, or fandoms like Harry Potter and Marvel Comics. I think this is one of the mistakes that folks who study this can make, folks who want to dedicate their lives to combating the scariest parts on the internet: Don’t weigh the worst stuff heavier than the light stuff. Actually, the funny and life-giving stuff is also how you narrate the scary stuff.

I think you're doing yourself a disservice as a researcher if you're only looking at the worst parts of information warfare. But I guess that is also why a lot of us studying the internet have a really dark sense of humor. I think Mark Twain said there is [no humour in heaven](#).

Q: Looking ahead to the 2026 midterms, what do you expect to see in terms of information warfare?

Danielle Tomson: The thing that's different this time around is that there's less novelty around some of the narratives around election integrity. The repetitiveness now is actually getting boring, and the internet hates boring things. And the fact that we're talking about past elections being "stolen," when Trump himself is president again ... there's a certain basic logical fallacy there that even folks on the internet are pointing out. At a certain point, you have to just laugh that they're still talking about the same thing now for six years. You can predict what's going to happen, and that's boring — except that the implications for the commitment to this bit are really serious and dire.

However, there are new dynamics too, like prop bets and the role of Kalshi and Polymarket, and turning our breaking news environment into a space where people can use different kinds of inside information to make money. My [colleagues have written about this](#) in collaboration with the Brennan Center. And if you want to think of Kalshi and [Polymarket](#) in these kinds of spaces, it's doing on a more public level what hedge funds have done for a much longer time in moving markets. The role of AI is new, too, as people go to these antisocial forces for information as opposed to pro-social ones like social media. So those things are different.

Q: What advice would you give to someone wanting to do what you do?

Danielle Tomson: Find God! Kinda not joking. I think a lot of people get into studying communication as a way of studying some of the intangibles of life. As a comms scholar, I'm interested in how people express their fears, desires, stakes, and needs to each other. Sometimes that is dialogue, verbally, and sometimes that's through force or other kinds of nonverbal communication. And I think when you're interested in communication, it usually means that there's something that you're fundamentally interested in that isn't entirely visible, with deeply personal or spiritual dimensions. And the sooner you identify that, the deeper the impact on your work.

Never lose sight of that bigger "Why?" Something that I've learned from MAGA influencers is that they help their audiences answer that bigger "why" question. What is a good life? What is the purpose of government? What is happiness? What is a healthy life? They attempt to answer those questions in a very accessible way.

As stewards of public knowledge and knowledge generally, we can't lose sight of that obligation either. Yes, you have to keep up to date on new methods and skills and academic papers and professional associations and all that. But don't lose sight of that bigger "why," because that's what's at stake right now: people asking those big questions and other people being willing to take the risk in answering them.

So don't be afraid to take the risk of trying to answer the big questions.

6. A Reporting Guide to AI-Generated Intimate Images

By Kaylee Williams

Kaylee Williams is a Ph.D. candidate and former Tow Center research fellow at Columbia University's Graduate School of Journalism. Kaylee's research examines technology-facilitated gender-based violence, and she is currently writing her dissertation on generative AI and nonconsensual intimate imagery. Prior to her doctoral studies, Kaylee was a research fellow at Harvard University's Shorenstein Center for Media, Politics & Public Policy, where she investigated coordinated disinformation and cyberharassment campaigns. She is now working as a lecturer in the Media Studies major at University of California, Berkeley.

In this article, Kaylee discusses the rise of sexually explicit deepfakes and AI-fueled “nudification” apps — new tools in the information warfare armory that are being used to predominantly target women across the globe, from prominent politicians and celebrities to classmates and colleagues. She explores the threat posed by this technology, and explains how reporters can cover this subject with more accuracy and empathy, while better protecting themselves and their colleagues from associated harms.

Using AI to generate sexually explicit images of real, nonconsenting people may not immediately register as an act of information warfare. While the behavior may be widely understood as potentially illegal, unethical, and unquestionably creepy, AI-generated intimate images are rarely characterized — in news coverage, policy analysis, or public discourse — as a variety of disinformation.

Journalists tend to focus their coverage of so-called “deepfake pornography” on the individual harms inflicted on women and children — two groups who [studies have shown](#) are frequently targeted for various forms of image-based sexual abuse (IBSA). And rightfully so. [Academic research](#) has shown that victims of AI-enabled sexual exploitation, including IBSA, often suffer immense psychological, social, and financial consequences after learning they've been targeted, including post-traumatic stress disorder, isolation from loved ones, and job loss.

However, in addition to the horrific personal impacts that this content generates for many individual victims, I argue that AI-generated intimate images also contribute to a concerning society-level phenomenon that threatens civil liberties and democratic norms on a much broader scale.

Today, [there exist hundreds of publicly available apps](#), websites, and other digital tools that can create sexually explicit images and/or videos of any person, for free, with a few clicks. While several jurisdictions in the [United States](#), [Europe](#), and [Asia](#) have sought to outlaw these tools, major platforms like Facebook, X, and Google have continued to [advertise their capabilities](#), and have largely [failed to mitigate](#) the [spread of their abusive outputs](#). xAI, the Elon Musk-owned creator of Grok, has [recently launched](#) a lawsuit to block the passage of a Minnesota law banning apps that enable users to generate intimate images of real people on the grounds that the proposed ban violates the company's First Amendment rights.

All of this has resulted in the rapid escalation and normalization of gendered sexual exploitation in general, and the use of sexual humiliation and shaming to [undermine and silence women's voices in particular](#). A growing body of academic literature and journalistic reports show that women [politicians](#), [celebrities](#), [journalists](#), and other prominent public figures are among those most frequently targeted for IBSA.

[Numerous studies](#) have found that victims of IBSA and other forms of online harassment are more likely than non-victims to reduce their online presences either by pausing use of social media platforms, or deleting their accounts in an effort to prevent further abuse.

Knowing this, it is no coincidence that [two dozen Congresswomen](#), many women heads of state, countless local candidates, and a variety of other women in politics and pop culture are among the best-known victims of this emergent form of abuse. After learning she'd been depicted in a deepfake sex video during her campaign for the Northern Ireland assembly in 2022, candidate Cara Hunter faced [public shaming](#) and isolation so severe she told her husband, "I don't care if I'm elected or not. I just want this to be over." In January 2026, Argentinian journalist [Julia Mengolini told the Committee to Protect Journalists](#) that AI-enabled abuse and other harassment has made her consider leaving the profession.

In one particularly vulgar case from 2024, a meme of Vice President Kamala Harris depicted the then-presidential candidate kneeling on her hands and knees, mouth agape, surrounded by the caption, "Kamala can't talk right now. She's at a baby shower." The synthetic image circulated repeatedly on X, Reddit, and Facebook over that summer before [eventually being displayed on a billboard](#) in Ohio as part of a Trump campaign ad just weeks ahead of the election.

The company that approved the billboard later apologized, but the use of the image as a campaign ad reveals the misogyny that underpinned its creation. By depicting Harris in a position that many would consider demeaning and feminized, the creator (along with the person who commissioned the ad) implied that she was unfit to be president.

But the image also served as a warning. By dehumanizing Vice President Harris — the only woman to hold the second-highest office in the US government — in this particularly gendered way, the image communicates that *no woman* should expect to avoid public sexualization and ridicule if they choose to publicly engage in the political sphere.

That is to say, by activating long-standing biases around women’s sexual respectability, AI-generated intimate images contribute to an ecosystem in which women cannot freely and equally participate in public discourse without fear of being targeted for graphic or humiliating sexual exploitation. In effect, women’s political expression and representation in public life is increasingly disincentivized.

This chilling effect is what defines synthetic nonconsensual intimate images (NCII) as a potent, if unconventional, form of information warfare. Rather than attempting to confuse or push audiences in a particular ideological direction, these gendered attacks chill women’s speech and discourage their participation in public life by making their public visibility feel unsafe, untenable, or simply not worth it.

What follows is practical guidance for covering this issue with journalistic rigor and respect, starting with why gender must be treated as foundational to this particular manifestation of information warfare.

Gender Must Be Central, Not Incidental

There is [widespread consensus](#) among online safety experts and scholars that women and girls make up the vast majority of synthetic NCII victims. A [2023 study cited by UN Women](#) reports that up to 90 percent of synthetic sexual content online at the time featured women, while [my own research](#) reveals that many of the most popular nudification apps online today are *only* capable of generating intimate images of female-presenting subjects.

Despite all of the strides that women have made toward gender equity in politics, the workforce, and the domestic sphere over the last century, we still live in a society that regards women’s bodies as fair game for public ridicule, sees expressions of feminine sexuality as morally and professionally discrediting, and regularly reduces women and girls to sexual objects for male consumption and enjoyment. Reporting should situate synthetic NCII within this broader cultural reality and trend and not treat incidents as one-off interpersonal disputes.

For many, the first step will include making thoughtful choices about the phrases and labels used to refer to abusive content. Although “deepfake pornography” has largely become the dominant term for synthetic NCII — both colloquially and in mainstream media coverage — victim advocates and scholars of gender-based violence stress the importance of not conflating IBSA with legitimate

pornography, which is legally protected and carefully regulated in an effort to protect sex workers and restrict access by minors.

Furthermore, the use of more harm-centered terms like NCII (a subset of IBSA) “emphasises the links between the non-consensual use of private sexual images and other forms of sexual violence,” [wrote legal scholars Clare McGlynn and Erika Rackley in 2016](#). “It locates this form of abuse on the continuum of sexual violence, alongside other forms of abuse attacking women’s sexual autonomy, identities and integrity.”

Ethical and Respectful Handling of Abusive Materials

Journalists covering synthetic NCII will encounter visual materials that are disturbing, degrading, or otherwise abusive. Even brief instances of viewing such material can produce vicarious trauma for the reporter, as well as unnecessary exposure for the person who has already been victimized.

A useful starting point is to regard synthetic intimate images as evidence of potentially criminal activity, even when the legal boundaries are unclear. Thanks to the [2025 Take It Down Act](#), the distribution of nonconsensual sexual content is now considered a federal crime in the United States and punishable by up to two years in prison. Local jurisdictions, including some states, carry even stricter regulations, with limited carve-outs for journalism and research. Reporters need to understand these legal boundaries before viewing, storing, sharing, or publishing any such material, including how their jurisdiction treats possession, redistribution, and publication.

With all of this in mind, journalists should view abusive content only for as long as necessary to verify specific claims, and then move on. Minimizing exposure benefits both the victim and the reporter. NCII-related laws also have implications for the storage and exchange of materials between journalists. Screenshots and other records should be kept only when they are necessary for reporting, secured behind encryption or password protection, and separated from personal photo libraries.

When it comes to working with known victims, reporters must be transparent with the person depicted about what content has been found and how it will be used in the newsgathering process, and in publication. Showing someone an abusive image (either of themselves or someone else) without warning, or reproducing it in a story without consultation, can lead to re-traumatization and unnecessary harm.

These considerations extend to how the material is described in print. The language of the story should focus on the *violation* that has taken place rather than on the anatomy or appearance of the person depicted. Neutral, clinical descriptions communicate the facts without reproducing the logic or the “appeal” of the abusive media. The same principle applies to visual presentation. Images of a victim,

even when blurred or partially obscured, should not be used as thumbnails, banners, or other promotional materials that circulate independently of the story. Editors and reporters should strongly deliberate the news value of publishing any visual material, even when obscured. In cases where reproduction is essential, identifying features such as faces, tattoos, or other distinctive markers should be removed or censored to reduce the image's traceability.

Material that appears to depict minors should never be searched for, reproduced, or stored. In some jurisdictions, even viewing or taking screenshots of sexual abuse material featuring children — AI-generated or otherwise — [can trigger legal liability](#). If at all possible, reporters should consult a lawyer prior to launching any investigations involving child sexual abuse material, and report individual instances of abuse as [mandated by local law](#).

There are forms of newsgathering that should be avoided altogether. Nonconsensual subjects should never be used to “test” or experiment with nudification tools. Even using one's own image for that purpose carries risks, since many of these systems retain inputs for training data. When experimentation is necessary to understand how a tool functions, it should be done with images that cannot be connected to a real person, such as artistic works in the public domain that depict fictional characters.

The Importance of Rigorous Digital Archiving

One of the defining features of the online ecosystems in which synthetic NCII circulate is their ephemerality. Abusive forums and tools frequently disappear without warning, only to reappear under new names. Similarly, individual posts are often deleted the moment they attract scrutiny. Platform policies shift quietly, enforcement practices change without public explanation, and content that was easily searchable one day is inaccessible the next. For journalists encountering evidence of wrongdoing *after* the initial harm has taken place, the result can be a landscape in which the abuse is widely referenced, but difficult to locate or verify.

This volatility is not incidental. It provides a structural advantage to those who create, distribute, and profit from abusive content. The longer a reporter takes to verify a claim, the greater the chance that the underlying material will be removed or relocated, allowing both the perpetrator and platform to avoid oversight and legal accountability.

In order to verify and preserve evidence of abuse, journalists should capture extensive screenshots, URLs, metadata, time-stamped notes, copies of platform terms of service and/or community guidelines in force at the time, and any other records that might be used to reconstruct the digital environment in which the abuse originally appeared. Together, these records constitute a rigorous

archive of events that can substantiate individual reports of abuse as well as attest to the efficacy (or lack thereof) of the safeguards that were supposed to prevent it.

These archives preserve the existence of the offending material, the context that made it discoverable, and the timeline that shows how long it remained discoverable online. In addition to the abusive posts or images themselves, reporters should document the pathways a user would have taken to discover it, noting the search terms used, menus clicked, account status required, whether automated recommendations surfaced the material, and whether any community notes, fact-checking labels, or sensitivity screens were applied. Where possible, preserve the surrounding threads or conversational context, the alleged perpetrators' profile(s), and any adjacent references to specific image generation tools or affiliated digital communities. These details are often useful when trying to establish the perpetrator's motivations, or uncover the technological methods that went into the material's creation.

When material is removed or links are broken, document that too. Evidence of strategic or delayed removal can be as important as evidence of initial circulation, particularly when platforms claim to have intervened on behalf of victims.

Don't Fall for Big Tech Marketing

Another pattern in the development and marketing of generative AI systems is the mismatch between stated safeguards and models' observed behavior. Particularly during the periods following the public exposure of some egregious oversight, new guardrails are often announced by the company under scrutiny, and technical fixes are framed as assurance that the underlying problem has been solved or mitigated.

In turn, the media will often promote these changes in its coverage, subtly commending the companies for seemingly addressing user complaints before moving on to other stories. Google, for example, earned a wave of laudatory coverage in 2025 when the company [announced](#) a new partnership with the nonprofit developer of [StopNCII](#) — a free tool that uses hash technology to detect previously reported abusive images — despite the fact that the tool was largely already considered the industry standard at the time, and that more recent coverage reveals that Google [continues](#) to host “nudification” apps dedicated to generating sexual abuse content on its app store.

However, when an AI company or digital platform claims that new guardrails, improved detection systems, or policy updates will help prevent abuse at scale, those claims should be treated as testable fodder for reporting, not as newsworthy in and of themselves. This means comparing the capabilities and limitations of a given tool both before and after the implementation of the supposed intervention, to see for yourself whether the proposed change has actually resulted in meaningfully different outcomes for users.

Coverage of X’s proprietary chatbot, Grok, from early 2026 offers a clear illustration of why this kind of reporting matters. In January, journalists and researchers [showed](#) that users were able to generate nonconsensual intimate images of real people — including material that appeared to depict minors — at alarming rates, prompting investigations by regulators and law-enforcement bodies in multiple countries. After a wave of public outcry, the [company announced](#) that it had implemented technical measures to prevent the tool from altering images of real people. But [subsequent reporting demonstrated](#) that the restrictions were only partial, and that the bot continued to produce nudified images at users’ requests for weeks after reporting that the problem had been fixed.

Without contemporaneous records of what the system could do over time — which prompts worked, which features were still live, when restrictions were introduced, and what content remained visible, for example — the Grok incident could be mistaken for a company dutifully adjusting its product in response to public feedback. In reality, the abuse continued for weeks, the changes arrived slowly, and nudified images are still circulating through parts of the platform, even after new safeguards were introduced.

Rigorous, accountability-focused journalism makes visible the gap between public promises and delivered results. The story becomes one of governance, financial and political incentives, and corporate accountability, rather than spectacle or technological determinism. Seen in that light, covering synthetic NCII is not only about documenting abuse. It is about documenting how power is exercised in ways that make women’s public participation more costly and, in turn, undermine democratic norms.

This means tracing how design choices, moderation policies, legal frameworks, and business models determine who can remain visible without fear of sexualized punishment, and who is pushed to shrink away from public visibility. This approach places the rapidly-advancing technology in its proper context — as one element in a system shaped by people and companies that should be publicly named, questioned, and held to account for failing to protect users from harm.

7. Q&A: Brandy Zadrozny on Conspiracy Theories, Protecting Sources, and Protecting Herself from a “Depressing” Beat

By Emma Goldhaber

Brandy Zadrozny, a [senior enterprise reporter for MS NOW](#), has been one of the leading journalists covering politics and misinformation for the last decade. Originally trained as a schoolteacher and a librarian, Brandy has been a reporter for NBC News and before that *The Daily Beast*, covering stories on COVID-19 conspiracy theories, QAnon, election deniers, and other “[depressing](#)” aspects of internet culture.

In this interview, Brandy discusses how her beat has evolved over time, the effects of mis- and disinformation, building trust with sources, and the personal cost of covering stories like those she has broken throughout her career.

[This interview has been edited for length and clarity.]

Q: To start off, how would you describe your beat these days?

Brandy Zadrozny: Oh boy. That’s a great question. I think my beat is politics, misinformation, and the internet.

Q: How has that changed over time?

Brandy Zadrozny: When I first started in, I think it was 2013, the beat was the internet and politics. And we didn’t call it misinformation then, but, you know, “shenanigans.” And it was pickup artists and extremists and just weirdos on the internet telling lies and trying to influence society and politics. And over the years, those people have become very politically important and central to the way that we communicate, and the way that politics works, and the way this administration goes about its business.

And so, it’s changed a lot. There were like five of us doing this beat ten years ago, and now ... everybody’s a disinformation reporter! Misinformation online has become so rampant, and the peddlers have become so powerful, including the United States government. It’s just become all encompassing, I think. It’s everything now.

Q: Is there a key moment that you look back on that changed everything?

Brandy Zadrozny: Yes, I can think of three just off the top of my head.

One is the pandemic, obviously. Everybody shut in their homes. Everybody, scared, around one world event, and everybody looking to the internet for answers. What that did was it exploded ... it boosted a number of folks who had spent years laying the groundwork for misinformation around health.

People like Robert F. Kennedy Jr. became really supercharged during the pandemic. They grew, and so did the mistrust and distrust of doctors and the narratives that we got from, or I should say, around doctors and the CDC and the World Health Organization. And MAGA at the same time — including Donald Trump, even though he was behind [Operation Warp Speed](#) [the project launched by the U.S. government in May 2020 to speed up the development, manufacturing, and distribution of COVID-19 vaccines]. They really cultivated the folks who sort of leaned into that distrust. And so you had this alignment between anti-vaxxers, which really were on the left, and the right and MAGA folks. And so that — I’m using air quotes here — “health freedom movement” became a really activating part of MAGA.

What that led to was the ascension of Robert F. Kennedy Jr. as a political candidate, and then as a Trump ally when he dropped out, and now [secretary of] the Department of Health and Human Services. He’s been there [over] a year and, I would say, has totally remade public health in his image.

Another I would say is Elon Musk buying Twitter. There were many dominoes that fell in the wake of that purchase. What it did primarily was cut off one of the most reliable platforms for information that the country used in times of crisis, during elections, just to share journalism.

And what it turned into when Elon Musk invited white supremacists and literal Nazis back on the platform ... it promoted, by way of the algorithm, influencers over news organizations for information. It turned a really reliable information-sharing platform into a cesspool of hate and lies. And so that’s been pretty significant on this beat.

And then I would say the second administration of Donald Trump has been pretty significant. I think the people that he has surrounded himself with, especially in Health and Human Services, and in the Department of Justice, and Homeland Security, have really leaned into lies to promote their goals — to propagandize for their goals. We’ve seen that very much in the way that ICE uses propaganda. You can go on these accounts and they’re just ... sometimes I have to get my bearings, because to realize that these are government accounts, and what the propaganda on these government online accounts really looks like is meme warfare out of 2016. It’s internet garbage and in some cases, like the ICE accounts, it’s white nationalist imagery, and that’s been a strange thing to see. And we didn’t have that in the first Trump administration, not to the same extent. We’re really seeing it now.

Q: How has the information environment changed the job of journalists?

Brandy Zadrozny: I think it's made it 1) more difficult and 2) more imperative that people get it right. It's more difficult now to report on what the federal government is doing because so often, the federal government is bold-faced lying.

I used to joke that the beat was, "Hey, that liar is lying on the internet." And so I would go and debunk the lie and say where it came from and explain who was telling it and what impact it might have on certain communities. And now, every liar is lying on the internet at all times and in real life. And everybody is a disinformation reporter now.

And I think it's really hard. Not to toot my own horn. It's hard to be a disinformation reporter. It's hard to contextualize a lie, especially when it's coming at you like machine-gun fire. So I just think it's super, super hard. To be a good disinformation reporter, you have to be able to say, "This is not true. Here's how I know, and here's the damage that it does." And it's just not something that people are really keen on doing right now.

Q: What are the biggest challenges that you've faced when reporting on this beat?

Brandy Zadrozny: I think that this beat came with a load of harassment and online abuse and that made it really difficult to do the job at all times, which is why several people that have been on this beat are no longer on this beat. We've lost some good ones. And I think that very much takes a toll, whether it's because I often cover extremist events — and disinformation [that] powers extremism — they often go hand in hand.

And so, to see or to have to watch violent events all the time, and to have to report on the people who spread the disinformation that powers the hate that leads to these violent events. ... It's a depressing beat, generally. You have to often report on people who not a lot of people report on, like in the mainstream press, but they have huge online followings, and in some cases, real-life connections with extremist organizations that will try very hard to harass you or scare you. And so that is a part of the job that I did not sign up for, and that has been consistently hard.

With the broadening of this beat and the inclusion of lots of new people — again, we're all disinformation reporters now — I think that the harassment has spread out more, strangely. So much that it's far more common for journalists to experience that harassment.

Q: What do you do to manage risk and protect yourself, whether it's physical protection or mental?

Brandy Zadrozny: I've gotten much better over the years, and I do a couple things. I now practice good digital hygiene in a way that I may not have always cared about. My children aren't on the internet. My husband isn't on the internet. I don't mix my job with my real life. That's really important.

The second thing is I learned to compartmentalize in a way that I haven't always done, which is to say, sometimes it's physically the act of compartmentalizing between my job and my life. So if I'm watching something violent, or I'm watching or I'm doing research on Nazis that's disturbing, I will do it in a specific place at my desk, and I will literally say to myself, "This is not my life. This is not happening to me." And then when I'm done, stop and close my laptop and go do something else.

There was the New Zealand mosque shooting that was very obviously terrible, and I was [reporting on it](#). It was during dinner time, though, so I was watching it live, and I had to feed my children at the same time. I had earbuds in, and I'm watching it, trying to write about what I was seeing, and then also cooking for my kids and hearing them in the next room. And I realized at that point, that is not a way to do this work. That [it] was a failure on my part, and I had to correct it.

So now I'm pretty regimented about when I do the parts of my work that aren't nice and where I do them. And I compartmentalize my feelings about if I'm at the center of a harassment campaign online because somebody didn't like something I wrote about them, which happens, you know, every other week. I'm not on X anymore. I mute harassing threads. I just turn it off in a way that I find very helpful.

I also have hobbies, which I know sounds really silly, but you cannot make this your whole life, especially if this is the beat. You will burn out. And so I run, and I knit, and I'm with my children, and I do things that are not this job, often.

Q: Thank you. That's extremely helpful. Doing a hard pivot, what story are you most proud of?

Brandy Zadrozny: Oh my God. I think, as journalists, we all want to have an impact. And I think there are two, and they're totally different, but they each explain kind of a genre that I think is impactful. A lot of the disinformation beat is reporting on people who the world doesn't know, or that the world doesn't understand how impactful they are. Renée DiResta, I think, calls it "invisible rulers" [in her book](#).

So there is the story of how Jim Jordan had this [committee on the weaponization of social media](#). And what he did is he pulled up researchers and subpoenaed tons of information on researchers and that's where all the Twitter files were so-called "investigated," and where the government told this false story, this story of the conspiracy of the ... it's called the censorship industrial complex.

And I knew that there was this one guy who was kind of the brains of it, and his name was Michael Benz. He was this nobody who's worked as a lawyer for a little bit. He was a dancer, and a piano player, and I found out that he had made all of this racist content. He was a racist YouTube vlogger, and he had made, for years, just super racist antisemitic content on YouTube before wiping his channel to go work for the federal government under Trump.

And I outed him. Basically, [I wrote a story](#) that says, “Here’s who this person is and why he matters.” And Michael Benz has gone on to be the brains behind the dismantling of USAID. He is now a very well-paid content creator for a right-wing media ecosystem that spins up conspiracy theories. But there is one article that will forever be atop his Google results page that says: Here is who this person is. Stuff like that is really important, and so I’m proud to have done it.

And the [other story](#) that I really like, because it was explaining why people believe things on the internet in a way that is nonjudgmental, and maybe reveals something about the way that we believe things. ... I read the story about this woman who was in a free birth Facebook group — a free birth online community — and she ended up relying on it, and she said, “brainwashing” herself through this group to not seek medical care, even though she was forty-four weeks pregnant. And she lost her baby.

And I just spent a lot of time with her, and dove down that rabbit hole with her. And I get letters still from women all the time saying again that they looked up this pregnancy group and found her story. So, something that helps people navigate their real lives and is sensitive to the subject in a way that — you know, I’m still friends with this woman that I profiled — I think makes me really proud.

Q: For interviews like that, where it is such a sensitive topic, or even in the space of interviewing people about their beliefs and in this general space of mis- and disinformation, how do you gain people’s trust to do an interview with you?

Brandy Zadrozny: I have a couple of things that I do.

The first is that I don’t give up. I have to go back to people over and over again, and sometimes things change. Like with that woman I had seen, I was watching these pregnancy groups. It was kind of an obsession of mine, and I saw what happened to her in real time. So you know, six months after that happened, I reached out to her and said, “Hey, I saw this experience. I’d love to talk to you.” Didn’t hear back. Several months after, I reached out again, I’m like, “Here’s the stuff I report on. Here’s the kind of thing that I do. I’d just love to talk to you on the record or off.” I always offer on the record or off at first to a subject like that.

And then, before we actually start reporting, [and] somebody agrees to talk to me, I have this, I call it the Miranda rights [that] I go through with them — this is before they talk to me, and then after they talk to me, but before we publish — [I] say, “Here is the story.” And I don’t give it to them, but I will often read huge passages from it. And I say, “Here’s the story, let’s talk about what you’re feeling before this is published. And let’s think of the consequences you might face, right? Like, if we use your middle name for this, [will] somebody still be able to find you? Might your family members know that this was written about you? A job, if you’re using your name, will an employer be able to Google this about you? Will you be forever known as whatever?”

And so I find that a lot of times people will say, “Actually, yeah, no thank you.” And I’ll be like, “I totally understand if anything ever changes, or let’s just talk off the record in a way that I can hear your

story and it'll inform my reporting going forward. But you don't have to put your name out there or tell your story on the record."

Giving people an out and then letting them know it's their story to tell, it's really important that we all do that.

I did this story once about a guy who went to the Capitol on January 6, and he had totally fallen into QAnon really badly over the last couple of years. He went to the Capitol expecting something to happen, and then he reached out to me, and he shared his entire computer history with me. His Google folders with me, with all his writings, his Facebook account, which showed what he was looking at, who he was communicating with, all of his posts, he gave me everything. And I spent a month writing this story about how he had fallen prey to this conspiracy theory, and how he pulled himself out.

And as I was reading him parts from his story I had written, he said, "I can't do it." And so he pulled out after I had put in all this work. And I was like, "No problem. We are still fine; it's your story. If something changes, let me know."

And a year later, he reached out to me, and it was the anniversary then of January 6, and he said, "I'm ready to tell my story, if you still have any interest in telling it." And so we did. We [published it a year later](#). And I think that, if you're a normal, nice person, then people will want to tell you their stories.

Q: What's your process of taking a large topic, like disinformation, and turning it into a compelling narrative story?

Brandy Zadrozny: Beats me! I think I feel like every single story, I totally forget how to do this job, for what it's worth. So I don't know. I think you need to have a good character to tell a good story that sticks with people. And you need to get somebody to tell you their story. And as we just discussed, that is not often easy.

The other thing is to explain something to someone: to answer a question. I was just telling an editor this the other day... I was like, "But this doesn't answer a question." If it doesn't answer a question, then I don't think we should be doing it. Or, that's not my beat, right? We have to explain, we have to answer a question.

Q: What advice would you give new journalists who want to work on this beat?

Brandy Zadrozny: I would say that there are more stories than there are journalists out there right now. And the trick is to find a story that no one has told or finding an angle that no one has seen yet. I read in [Julie K. Brown's book](#) on the Epstein affair, she had this anecdote where her editor told her, "If you see a pack of reporters, run the other way." And I think that's true. Not just in actual events, but in practice of journalism. Originality and something different, it makes you indispensable.

Q: What advice would you give them about personal risks or impact?

Brandy Zadrozny: Well, first it's digital security. I think before you enter the workforce, clearing out your old pre-journalist life is really helpful.

At one point I felt a real connection to my online life, but once I got rid of it, once I cleaned up and stopped digitally hoarding, I actually didn't miss anything. And I feel much safer knowing that when the mob comes for me — and they will again, and they will for you — you've done the best you can do to cut off their access to you.

And take care of yourself. The job cannot be everything.

8. The Other Side of the Recorder

By Anika Collier Navaroli

***Anika Collier Navaroli** is an award-winning writer, lawyer, and researcher whose work covers journalism, social media, AI, trust and safety, and tech policy. She is the Craig Newmark assistant professor of professional practice, director of the Craig Newmark Center for Journalism Ethics and Security at Columbia Journalism School, and a technology [columnist](#) at Columbia Journalism Review. Over the past decade, her work has ranged from law firms and think tanks, to advocacy organizations and senior policy positions at Twitter and Twitch.*

Here, Anika shares her experiences of being a whistleblower at Twitter, exposing trust and safety failures leading up to the January 6 attack on the US Capitol and the suspension of President Donald Trump from the platform. The article also explores her perspective on telling her story through the press and offers practical guidance for reporters working with sensitive sources, including four key lessons she gleaned from her time on the other side of the recorder.

Two years ago, on a balmy San Francisco late summer day, I arrived at my call time for an interview for a documentary about the company that used to be called Twitter. It wasn't my first interview, but by the time the director called "Cut" nearly four hours later I knew it would be my last.

Weeks before, I had spoken with the people making the documentary. I had become weary of talking to journalists about my time working at Twitter, but I agreed to discuss participating in this film because it had been commissioned by reputable, well-known news networks in the United States and abroad.

I explained to the producers that I had clear boundaries around what I was willing to speak about on camera. I said they could use the [hundreds of pages](#) of my Congressional testimony, or the [infamous video clips](#) from my depositions, to get into the details of the preferential treatment that Twitter had afforded to the president, as well as the warnings I gave to Twitter's leadership in the run-up to the January 6 attack, and my [insider view](#) of the momentous decision to finally deplatform Trump. But I really did *not* want to retell, and thus relive, the vivid minute-by-minute memories of January 6 that I had been trapped in for years that felt like lifetimes.

Columbia Journalism School

So it came as a surprise when I arrived on set and was pulled aside by those same folks who had agreed to respect my boundaries. I was told that they had decided it would be better for the documentary if I spoke directly on camera about the things I really didn't want to talk about.

It was a classic [bait-and-switch](#) move.

But what could I really do? I had already signed the standard release forms necessary to appear in any TV production. And the whole crew was waiting. So I did the interview.

A few months later, after the 2024 US election put Trump back in the White House, I reached back out to the documentary's producers. I told them that given the changing political climate in the country — and my previous experiences in dealing with direct [threats to my safety](#) — I wanted to discuss how my interview would be used.

When we got on the Zoom call, I was told that I didn't have to worry. While the earliest cut of the film began the series with footage from my interview describing my day working at Twitter on January 6, the media company's executives had given notes that were being implemented in the final edit. Apparently the executives wanted less footage of me — the person who had actually done the work, experienced the event, and lived through the consequences. Instead, they wanted more airtime from the network's talking-head contributors — who had no firsthand knowledge of the events and had risked nothing to talk about them, but who were [reportedly](#) being paid \$250,000 annually for their pontifications.

I was bewildered. As a human, I felt happier and safer that the most sensitive parts of my interview were being cut. But as a trained journalist, I was pissed to learn that the cuts were not being done to protect a source or for solid editorial reasons, but rather because the network executives wanted to showcase their more flashy contributors.

In the end, I didn't watch the documentary when it aired in the U.S. Nor did I hit play when it made its way to streaming services. And I have turned down every documentary request that I have received since.

Despite that anecdotal lede, please know that I am not blaming my decision to end my whistleblowing journey on one bad interview or journalist. It was more of a death-by-a-thousand-cuts situation.

Whistleblowing shattered many of the foundational beliefs that I held. It also imposed a huge personal toll. For one, there was the constant stream of threats to my life that upended my sense of safety and

[sanity](#). More existentially, my experiences of telling my story in public had fundamentally shifted the way that I viewed the media.

As a trained journalist and media lawyer, I had believed in some moral notion of “Truth.” It was the guidance behind much of my decision-making. I believed in an almost ethereal ethical code that bonded together the institution of journalism, as naive as it may sound.

But then there was the primetime interview with a well-known journalist, with whom my lawyer had discussed the parameters of what I was legally allowed to speak about before I agreed to come into the studio. Yet, under the camera lights, and while trying to not break a sweat, I found myself having to navigate my way out of questions that put me in the exact legal jeopardy I had sought to avoid.

Then there was the Pulitzer Prize-winning journalist who boasted of their degrees and brazenly pumped me for sources.

And there was another documentary interview that was so unexpectedly contentious that when the camera cut for a break my immediate reaction was to ask the journalist, “Are you serious right now?”

For the first time in my life, I found myself understanding [critiques](#) of “the mainstream media.” I too had discovered that I couldn’t exactly trust the biggest names in news. The reverence with which I once held the profession began to wither.

At the same time, I was facing additional repercussions for my whistleblowing. I was once known within my field for being good at my job. At Twitter (and subsequently at Twitch too), I had written thoughtful, high-stakes, enforceable platform policies at a relatively quick speed. I knew that my reputation would change after I spoke out. But I hadn’t fully realized that I had now become a liability in an employment field in which the key requirement is keeping secrets.

As I looked around, I noticed that my career prospects within the technology industry were dissipating at an expedited rate. Yes, some companies were willing to consult with me under arrangements that I did not publicly disclose my work with them. But when I applied for permanent roles — that I was extremely overqualified for, perfectly qualified for, or where I personally knew the hiring manager — the result was always the same: I never even got a screening interview.

It’s an experience that, while embarrassing, isn’t unique. Whistleblowers, especially those of us from Big Tech companies, have faced tremendous consequences for speaking up.

Yaël Eisenstat, Facebook’s former global head of elections integrity ops, wrote publicly about the company’s political ad-targeting tools in 2019. Now the director of policy and impact at Cybersecurity

for Democracy, she told [The Washington Post](#) that afterwards, “I knew it, like, in my gut ... I had been blacklisted.”

Sarah Wynn-Williams, the former director of global public policy at Facebook, wrote a memoir, *Careless People*, about her time at the company. The book spent weeks on *The New York Times* best-seller list, but during those weeks, she was [barred](#) from promoting or distributing copies of her book, thanks to a court order obtained by Meta, who called its claims false and defamatory. The company went so far as to pursue legal fines that have placed her on the [brink of bankruptcy](#).

In December 2022, Twitter, under the new ownership of Elon Musk, engaged in a new scheme: a targeted disinformation campaign to discredit many of its former employees, myself included. The so-called “[Twitter Files](#)” released out-of-context Slack messages and emails from years prior to weave a fantastical farce of conspiracy and collusion. The published lies, along with employee names and contact information, led one former colleague to [flee](#) for his life.

Ellen Pao, the former interim CEO of Reddit, also experienced the impact of [lawfare](#) and harassment campaigns when she sued her former employer, the venture capital firm Kleiner Perkins, for discrimination. Years later, she talked to a *Harper’s Bazaar* reporter who interviewed several whistleblowers (including me) about [their experiences of what happens](#) after they’ve spoken out. “There is a huge change in how you view the world,” Pao said in the article. “There’s a huge change in what your opportunities are and how people see you.”

Given how I started this essay, the irony is not lost on me that of all the places that I would land after my whistleblowing journey, I’ve ended up working at a journalism school; let alone at my alma mater, Columbia University.

After two years as a fellow at the Tow Center for Digital Journalism, this year I was named the Craig Newmark assistant professor of professional practice and director of the [Craig Newmark Center for Journalism Ethics and Security](#) at Columbia Journalism School. Part of the role is to provide critical education about ethics and the real-world implications for journalists navigating the constantly changing media landscape.

I’m learning to make peace with being a case study in journalistic ethics. This semester, I’m on the reporting syllabus to talk to students about interviewing whistleblowers. I’m also teaching an Ethics Essentials course, where I have the honor and responsibility of guiding students through the principles and practicalities of our chosen profession, including how to navigate sensitive sources.

I plan to ask students, “Have you ever been on the other side of that recorder?” And then I’ll candidly speak about many of the interview experiences I’ve written about here before ending my presentation with a slide that outlines a few simple lessons for working with sensitive sources:

1. It may seem simplistic, but journalists must remember that sources are humans. They may have access to sensitive and sensational information that will make headlines and change history, but they are also people. Treat them the way you would want yourself or your family members to be treated.
2. Journalists shouldn’t be self-righteous in their reporting, especially with vulnerable sources. Most people have no idea how journalism actually works. Be willing to break it down and explain concepts like levels of attribution. Also be willing to negotiate interview boundaries beforehand that allow sources to feel safe. Then stick to those boundaries.
3. Fact-check quotes with whistleblowers. It’s an easy way to ensure that journalists have recorded details correctly and will relay that information accordingly. It also gives your source insight into what portions of their interview will be revealed to the public, so that they can prepare for any backlash or safety concerns.
4. Remember that while publication may be the end of the story for the journalist, it is often only the beginning of the journey for the whistleblower.

Despite my thorny encounters, journalism is where I’ve found my intellectual home. I’ve learned that it is a field that still embraces people who tell the truth. And by working to shape the future of the profession through those who will follow me, I am hoping that the next whistleblowers who come forward will have a better experience than I did.

9. Q&A: The Insider's Michael Weiss on war reporting, intercepted data, and the perils of investigating foreign intelligence services

By Stuart Anderson-Davis

Michael Weiss is an investigative reporter, author, and media commentator who specializes in war, diplomacy, and espionage. He honed his reporting skills covering the Arab Spring and the Syrian civil war before co-authoring the *New York Times* bestselling [ISIS: Inside the Army of Terror](#). Michael is a regular expert contributor on foreign affairs for the likes of *MS NOW* and *The Bulwark*. He writes the [Foreign Office](#) Substack and co-edits [The Insider](#), an independent online publication specializing in journalistic investigations, fact-checking, and political analysis. In this Q&A, Michael discusses his unusual route into investigative reporting and the many challenges he's faced, from working with sources in the intelligence services to the threats posed by hacking and social media trolling.

[This interview has been edited for length and clarity.]

Q: How do you typically describe your professional role to others?

Michael Weiss: Investigative journalism with a bit of commentary and analysis thrown in. So I sort of wear two hats. I do deep-dive investigations into Russian intelligence operations and espionage. Sometimes I do war correspondence. So I covered the civil war in Syria for 10 years. I went to Aleppo in 2012. I covered the full-scale invasion of Ukraine and was in Kyiv in April 2022. But I also do commentary, so I offer my opinions on foreign policy, diplomacy, the state of the world ... so it's kind of an eclectic mix. Broadly, it's journalism. I'm not really bound by some of the protocols of, for instance, the *New York Times* or the *Washington Post*. ... I believe that fidelity in journalism is at record lows. People assume you've got an agenda, that you're biased or you're compromised in some way. I just come right out and say, "This is what I think, take it or leave it." I'd rather set out my stall and let people decide.

Q: Did you always want to become a journalist?

Michael Weiss: My dream job at the end of my university days was working for [The Onion](#). I wanted to do satire comedy, but I wasn't good enough at it, and that's okay. So I took a job as a paralegal to pay the bills and make rent, and I actually started to watch and follow [Christopher Hitchens](#), and became kind of intrigued by his work. ... He's [was a] war correspondent, but he's known for his opinions and his polemics and all that. I ended up taking a class that he co-taught at the New School, befriend him ... he became a very dear friend ... sort of showed me the ropes and introduced me. So my J-school was him! I got a job at an online start-up ... went to the UK, ended up working for a think tank, and funnily enough, when I was at the think tank, I ended up doing more journalism ... because I was covering the Arab Spring and focusing on Syria. I said, "Well, if I'm going to do research and create policy papers I need to go to these places and talk to people."

Q: Looking back at your time in Syria during the civil war, what did you learn from being in that type of environment? What were the biggest challenges you faced?

Michael Weiss: I realized early on that I would never be a good war correspondent, because I don't have the stamina. It's a very specific kind of mental and physical style, and emotionally demanding.

In terms of danger, I was embedded with a rebel convoy with their technical trucks and whatnot that was driving down an expansive highway. It was a turkey shoot, like any Syrian helicopter or aircraft could have just picked us off. That was a little risky, and probably not a smart thing to do, but I made it out okay.

The other mistakes I made with Syria were, I think, becoming too invested in the subject matter. Too emotionally attached to the story, which is always a dangerous thing, because then you end up advocating ... I think that there were elements [among the Syrian rebels] there that were very genuine about what they wanted, but they were too naive and optimistic about the course that their conflict was going to take ... and I think their optimism kind of got the better of me. I became an advocate for that, without necessarily seeing just how easily things could go sideways.

Q: How did that experience with the Syrian rebels eventually inform your understanding of the rise of ISIS?

Michael Weiss: I became a student of jihadism and started to anatomize what it was, and actually it was both a liability and an asset, because I knew the subject matter and I knew the people involved. Some of those people ended up joining ISIS. When they did that, I understood what motivated them to do it.

It wasn't this kind of brochure, five-star jihad shit. It wasn't about watching YouTube videos or necessarily even being radicalized. It was a human component to this. They felt traumatized, not just

by what was happening in the war zone, but also the state of geopolitics. They felt the United States was in a dark conspiracy with Iran and Russia to disenfranchise Sunni Muslims, and so I kind of understood the worldview.

If you fast forward 10 years, [HTS](#) [Hay'at Tahrir al-Sham], the former Al-Qaeda franchise, now runs the country. This was shocking and scandalizing to a lot of people. For me it wasn't, because I knew people who would join groups like this ... they were doing it out of pragmatism. These guys are the most combat-effective forces fighting the regime, they have the guns, they have the ammunition, they have the money. So that was the only game in town. My naivete of putting too much trust and faith in these people ended up giving me a kind of world-weariness.

Q: You've talked about the human component of reporting — meeting people, hearing their stories firsthand. Your approach seems quite different from those relying on open-source intelligence (OSINT), for example, and reporting from home or from a newsroom far away ...

Michael Weiss: I don't do OSINT. I have a great deal of respect for it, but one of the things that I think is a shortcoming is exactly this: people who don't leave their flat, they're staring at a computer screen all day trying to understand an incredibly complex and fraught situation based on YouTube videos or geolocation, and you don't get the human component doing it that way. If I were an analyst who only understood Syria based on data ... it's not going to explain to you why somebody joined a particular unit.

For example, in Turkey we'd meet guys who were joining Muslim Brotherhood-aligned rebel units, and I met guys who were drinking Efes beer, smoking weed, sleeping with Turkish prostitutes. I said, "You don't strike me as very [Ikhwani](#)." He said, "Yeah, no, we're not. What, am I gonna go join some bullshit Free Syrian Army brigade that exists only on Facebook, waiting for the West to give me pennies? These guys have the money." You get those personal insights by being *there*, and getting people to be comfortable with you and open up to you.

Q: One of your most famous pieces is "[Confessions of an ISIS Spy](#)" for the *Daily Beast*. How did you navigate the betrayal of a source turning into a member of ISIS?

Michael Weiss: One of the guys I've been talking around ... he was my fixer who brought me into Syria. So, he joined ISIS, and then he defected from ISIS. I felt a sense of betrayal, because this is literally somebody who I put my life in his hands to bring me to Aleppo ... and then when I hadn't heard from him, I assumed he'd been killed. No, it turns out he ended up joining this miserable organization [ISIS].

He wanted to tell a story. I met him in Istanbul, and over the course of three days, which was a very fraught and difficult three days, because on the one hand, I don't know if he's luring me to some trap to kidnap me, because, again, I don't trust this guy anymore.

He was part of what was called the *Amn al-kharjee*, so it was like the foreign intelligence apparatus of ISIS, who trained up the people who did the [Bataclan massacres](#). He was the translator, taking the instruction from the Arabic military commander ... and translating into French. It was very difficult for me, because again, the guy I'm relying on is somebody who had already betrayed me. I was in shouting matches with him ... I'm an American ... in Istanbul, having a shouting match with an ISIS spy, telling him, "Why the fuck are you doing this?" That was sort of surreal.

Q: You eventually introduced him to Western intelligence. How do you view the relationship between investigative journalism and national security interests?

Michael Weiss: I'm not going to pay him, but maybe Western governments could benefit from hearing what this guy has to say. ... So lo and behold, he ended up becoming an informant, both for DGSE [French intelligence service] and MI6 [British intelligence service]. We're at war with this terrorist organization; I'm not going to not act on an opportunity to maybe help the West defeat them. So I think my unique selling point as a journalist is I'm good at building relationships with sources. I don't seek to exploit, and I develop friendships. I develop, like, actual kinships, and it's similar, frankly, to being a case officer or intelligence agent.

I've managed to develop relationships with people inside intelligence organizations who tell me things that they should not. Knowing who I am, and what my personality is ... I don't set out to harm the United States or its national security. A lot of my journalism is focused on adversaries, particularly Russians, Bashar al-Assad, the Iranians, et cetera, and I think there's a degree of trust immediately knowing that I'm somebody you could talk to in order to further that agenda. Some of the stuff *The Insider* does ... we hack into Russian spies' email accounts, their Fitbits, their phones, we read their mail, so we operate almost like a sovereign intelligence agency. We just happen to publish everything that we acquire.

Q: Are there ethical lines you won't cross when coordinating with intelligence or law enforcement?

Michael Weiss: The only time we'll ever work dialectically with law enforcement or intelligence is if they're asking us, "Don't publish now, because the net is closing. We'll tell you when it'll be okay." ... We never kill a story ... it's always usually about speeding up publication or deferring publication. "Can you please not do this now? Wait a little bit, otherwise it's gonna make things difficult for us." I mean, God forbid, I should wake up and, "Oh, you published something and somebody got killed," or you know, the bad guy got away. ... That to me is going to weigh more on my conscience than having a chat

with somebody who's asking us to slightly inconvenience ourselves for the sake of stopping a crime or offense against my country.

Q: What are the tools that you and your team rely on to do your work?

Michael Weiss: This is how I do my work. I will meet you, and then I talk to [Christo Grozev](#) and [Roman Dobrokhotoy](#) [Michael's colleagues at *The Insider*]. They go into their little mind palaces. They have mountains of data, some of it is leaked by other hackers, some of it they get on the black market because everything is for sale in Russia, so they're the data guys. And we have a nice synergy, because what I bring to bear with the [shoe-leather reporting](#) and the sourcing fills in the blanks and provides the context.

I'll give you an example. When we did the stuff on [Havana Syndrome](#), it's actually very limited data that we had to work with. We had members of [GRU 29155](#) [a Russian assassination unit] in two different parts of the world. We could place one [agent], the son of the founding commander of the unit, in Tbilisi, Georgia, in 2021, when the wife of the chief FBI officer there got zapped while doing a load of laundry through the window. We found another guy ... in Frankfurt, Germany, in 2014 when another CIA officer got zapped inside the consulate. And the victims visually identified the two guys. We gave them a virtual line-up of Russian spooks, they said, "That's the one."

Everything else about Havana Syndrome was talking to victims, talking to people who study this inside the intelligence services. A lot of the people we were looking at had either served in Kyiv after the [Euromaidan revolution](#) or they were married to people who served in Kyiv, and they got hit after they left Ukraine. What I realized is one of the things the Russians were doing ... they wanted to counter American attempts to prop up Ukraine. They were taking pieces off the chessboard, which raises a whole lot of questions. How did they know where these American spies were being deployed?

Q: The implication being that there's potentially a leak or a mole?

Michael Weiss: Correct. And that's something that's been told to me by people who are still in government who have been investigating Havana Syndrome. So, anyway, this theory — what I call "[The Ghosts of Kyiv Station](#)" — has been ratified to me after the fact. So that was good journalism, if I do say so myself, putting the pieces together, talking to people, and then publishing something with a hypothesis attached.

Q: The sort of information that you're using to build your hypothesis — i.e. stolen information, personal data from the dark web — is that which a reporter at the *New York Times*, for example, wouldn't be able to use. Do you think this is going to change over time, as we see the type of impact that you can have when you incorporate that type of information into your reporting?

Michael Weiss: It gets to a point where people are able to do what we do and do it at scale, and it becomes supercompetitive. And I think the *New York Times* is going to say, "Well, we don't want to be left in the dust, yeah, we're going to have to change our protocols." For instance, at *The Insider* we have the opportunity to partner with other publications, but we don't partner with the *New York Times*, because they set the timetable for publication, they drive the car, and they dictate terms to us that are not amenable. Other publications, like [Der Spiegel](#), [Le Monde](#), no problem; [Delfi](#) in Estonia, no problem. I mean, European media is way ahead of the curve.

Q: With the type of work that you do — for example, the Russian investigations — how do you handle digital security and the threat of hacking?

Michael Weiss: I get spear-phishing attempts all the time. Ten years ago they hacked [Russian specialist author and former Moscow correspondent for the *Financial Times*] [David Satter](#)'s email ... and they started sending out Dropbox links to all of his contacts. I got an email from David with a Dropbox link, and I've known David a long time, and he doesn't know how to use this fucking stuff! I wrote back. I said, "David, what is this?" I get a reply, "Yes, Michael, this is me, no problem. Click the link." So the GRU [Russian Intelligence Service] is literally corresponding with me through his account! I had the wherewithal not to click anything.

Q: What about technology like Pegasus, where it doesn't require you to click something?

Michael Weiss: Very few things do I commit to email. Most of my communication is all Signal, and hackers are trying to get into Signal too, but from what I understand, if you're going to do end-to-end encryption, Signal is your best bet. I don't use WhatsApp. But I spoke about this with a hacker who had gone to work for an intelligence service. He said, "If they want to get you, there is nothing you can do." So, for them, it's just about return on investment. Are you worth going after?

Q: You've described being attacked on social media for your work. How did that affect you psychologically?

Michael Weiss: In 2015, just before the Russians intervened directly [in Syria] ... I wrote the first article in the Western press, saying the Russians are about to put boots on the ground, and then it became this sort of white dwarf moment of online vilification and disinformation. I had the Syrian

regime and the Russians collaborating to attack me because I was very outspoken. That took a psychological toll because I would wake up, I'd check Twitter, and it would just be a torrent of abuse.

Q: Did you develop any techniques to help you get through it?

Michael Weiss: Actually, Twitter developed a very useful technique, which I only discovered belatedly, which is that you can mute every notification or every engagement from people you don't follow. So just random trolling I wouldn't see, or I'd have to go out of my way to see it. Once that was taken off of my radar, things improved.

Q: Final question: What advice would you give to someone looking to follow in your footsteps today?

Michael Weiss: Knowing how the field has changed and knowing what direction it's headed in ... I don't know that I would choose this career. It's very volatile. It's extremely taxing on your mental stamina. It's exhausting as well, physically, because you have to be switched on at all times. I have to wake up at 5 o'clock in the morning to do television ... and that's not compensated, by the way. I'm doing that to stay relevant.

It's a very miserable profession in many, many ways. I haven't been back to Ukraine in two years ... not because I'm afraid, it's because my daughter is old enough to read the newspaper, and she's in mortal terror of me going to a war zone. I wouldn't be able to think clearly if I'm there while she's here in panic mode.

Journalism is a mixed bag. I enjoy it most of the time. But it takes a lot out of you, it really does.

10. Q&A: “It’s a game changer.”

Allie Funk on AI, human rights, and digital surveillance

By Emma Goldhaber

Allie Funk has worked for nearly a decade at the intersection of technology and human rights. Her career has spanned both civil society and the private sector. She previously led the Freedom on the Net report at [Freedom House](#), an annual study that assessed internet freedom in over 72 countries. In this interview, Allie discusses her path into the field, the effects of artificial intelligence on protecting human rights, and the growing surveillance threat to journalists.

[This interview has been edited for length and clarity.]

Q: How do you describe what you do?

Allie Funk: I’ve been in the tech and human rights field for about a decade now, and I’ve worn a number of different hats in my career. I spent most time in civil society doing a mix of research, advocacy, and policy. Most recently, in my previous role, I led the technology and democracy research at Freedom House, a democracy organization, the oldest in the United States, where I oversaw our [Freedom on the Net](#) report. I also worked with experts in the public and private sectors to advance human rights. So that’s everything from commenting on pieces of legislation to advising on a company’s risk assessment when rolling out new products in a particular market. And now I work in the private sector, helping ensure the internet is a tool to empower people.

Q: What first drew you to this field?

Allie Funk: It was really serendipitous. I was doing my graduate degree in human rights and was really interested in the ways in which counterterrorism policies impacted people’s fundamental freedoms, which at the time was under the Obama administration, and there were a lot of debates around the use of drones in wartime and the safeguards needed within government surveillance programs. That led me to an NGO, which was looking at providing legal representation to people who were indefinitely detained in Guantanamo, and trying to reform US surveillance law.

From there, I eventually found myself working on issues related to the internet and ensuring people could use it freely.

Q: What's been the biggest change that you've noticed over the past few years?

Allie Funk: I wouldn't find this the biggest change, but I think the thing that has struck me the most is the professionalization of the issues in the field. At the time when I was first entering — it was around 2015, so before Cambridge Analytica, for example — it was such a niche field. Many people weren't really paying attention to the impact of social media or how personal data was being collected and used by the private sector and government actors.

That has fundamentally changed. So many people — my family, friends around the world who work in other fields — are thinking about social media regulation, online privacy, the risks and opportunities of AI, and so much more. The number of people who are working on these issues, who care about them, and the expertise out there has just fundamentally changed.

Q: Is there a trend you've noticed that everyone is either ignoring or missing?

Allie Funk: Technology develops so quickly that attention jumps around really quick[ly] too, which means that a lot of problems don't get solved before another issue pops up that needs attention.

I worry this is the case with certain forms of censorship, such as website blocks. For years now, governments or other powerful actors have ordered that service providers block websites that host content they don't like, and often they do so with limited democratic safeguards. This isn't a new problem, but it's ongoing and happening globally in democratic and more authoritarian countries alike.

While there are definitely experts who are still focused on this issue, so much of public discourse has shifted to, for example, addressing AI governance. I think we need to be able to do both. Focus on longstanding challenges and opportunities for human rights and an open internet, and also turn our attention to more emerging ones.

Q: How has AI impacted your work?

Allie Funk: It's a game changer. So let me first start with my personal experience. AI has fundamentally reshaped how I do work. I'm more effective and efficient, and I've been able to offload repetitive work to automation so that I can focus on the more complex tasks, and spend my time engaging with people and organizations.

I'm consistently surprised by how much more I can get done in my day now with AI. It helps me prepare for meetings and events, conduct background research, synthesize and analyze datasets, and so much more. And my experience maps with what I'm hearing more broadly. It has been a game changer for this field: for conducting trust and safety work at scale, automating project management tasks, or identifying and plugging security vulnerabilities.

Conversely, I've previously conducted research into the risks of this technology. For example, I studied how AI could help scale digital repression by lowering the barrier of entry for who can conduct it. Years

ago, it used to be that the states with high technical and regulatory capacity were the ones that could be the most repressive. Today, AI makes that much easier.

From a surveillance perspective, previously it might be that you have an individual person who's scrolling through social media looking at activist profiles and identifying what they're working on. ... That [information] could be used to target somebody for arrest, or for harassment, or for even physical violence. Today, you could just use an AI system that is automatically combing through social media platforms and then comparing that data with what was collected from a biometric facial recognition system and from an internet service provider. Then AI tools can make inferences about a person based on that information. Where are they going to be next week, based on where they were last week? Who do they love, for instance, or who do they worship?

So I don't think there's one easy answer on AI. I'm personally excited about what it can mean for people's day-to-day lives because of how much it's impacted mine. But those benefits will only be realized if there is the right infrastructure in place and the technology is accessible and tailored to people's local realities. We do also need appropriate guardrails like security-by-default standards, democratic oversight, explainability, and humans in the loop.

Q: What role does surveillance play in silencing journalists, activists, or any kind of opposition figures before overt repression even occurs?

Allie Funk: I think surveillance has a clear impact on those surveilled and presents broader consequences for communities. First, you see in different countries around the world how data extracted through spyware or other surveillance technologies then ends up in a criminal case against a journalist or an activist. How data pulled from facial recognition is then used within a criminal case to say, "Oh, you were at this protest at this time. Here's a picture of you that we found." That's the acute impact: people who were targeted by surveillance technologies then facing direct repercussions for simply exercising their rights.

More broadly, it can also create an environment of fear where people might be more incentivized to self-censor over concerns that they're being watched. For example, a human rights defender who decides to stop doing their work because they don't want to be arrested or have their family doxxed. Or a student who is concerned that they may face retaliatory action if they speak out on social media about a particular issue. These people may not be directly under surveillance, but their concern that they could be can create a chilling effect on their willingness to participate in public life. This more nebulous impact is much harder to measure.

Q: What do people misunderstand about online surveillance?

Allie Funk: One thing that really irks me is [the] "there's nothing to hide" framing, And I think you hear this a lot, even within democratic societies. "If there's nothing to hide, there's nothing to worry about." But you know, privacy isn't about hiding, it's about dignity and having agency over how —

and to whom — you show yourself. It's also about future-proofing. You don't know, number one, who might be in power in a future government that could use data collected today against you in the future. Data collected from surveillance can also be misconstrued or be inaccurate. For example, some Americans have been misidentified by facial recognition and faced repercussions for crimes they didn't commit.

I also think about the way the data economy works, and the harms that can come from the collection of data by the private sector. In the US, for example, many people don't understand how data brokers can sell your data to the state, or to other actors, at another time for a different purpose than maybe you consented to originally.

Q: What are the most common threats that journalists face today?

Allie Funk: Globally, I would highlight the risk of spyware and other intrusion technologies. And that's because spyware is a really easy tool to get access to, and spyware has lowered the barrier of entry for surveillance for a lot of different bad actors. And particularly zero-click spyware that gives the deployer access to a person's device without the person having to click anything. My previous organization, Freedom House, and many other NGOs have done some incredible research documenting how this technology has been leveraged by governments who are targeting journalists in exile. So even if these journalists are in a more safe and democratic environment, they're still at risk of that surveillance from their origin states.

Rising censorship is another challenge journalists face. I would again highlight how this is particularly [evident] for journalists that are operating in exile and trying to get independent information to communities back at home, but are having their website blocked, [DDoSed](#) [distributed denial-of-service], or having their posts removed.

Q: Thinking about surveillance and repression on a global level, what are the key moments and developments that made the biggest impact?

Allie Funk: There are two big issues in privacy, data protection, and surveillance that were major turning points.

One was the [2018 Cambridge Analytica scandal](#). The harvesting of personal data from Facebook around the election to create hyperpersonalized ads got people aware that the data you give to the private sector — particularly social media platforms — could be used in attempts to sway your opinions. Folks had been talking about that generally, but this was the scandal that made it come to the forefront of the general populace.

The other big one that I would highlight was the [Snowden documents](#). When those were released, that really showcased how much the US government — one of the world's biggest democracies — was conducting surveillance. It raised serious questions about the rule of law and due process and fundamental freedoms. And that shocked [US] allies as well. The Snowden revelations also allowed

more authoritarian regimes to say, “Hey, the US is doing it, so it can’t be a problem that we’re doing it.” It served as a legitimization tool for disproportionate surveillance around the world.

Q: What steps do you take to protect yourself and your colleagues from hacking and other surveillance threats?

Allie Funk: The first one is just making sure you’re up to date on all your updates. That’s really important. It sounds annoying because they come all the time and I always have to delete apps on my phone to download them, but it’s key to do it as soon as they come out because they can be plugging for security vulnerabilities, such as spyware.

Second is to think about the messaging platforms you’re using and your security settings. I prefer Signal as my messaging app. That’s one of the best platforms for secure communication.

And then I would say more broadly, digital security can only get you so far, and individuals on their own can’t solve this problem. It really has to be a larger ecosystem approach that combines legal frameworks that prioritize security and privacy, and companies that build and help people adopt privacy-preserving technology.

Q: What resources and tools do you find particularly valuable?

Allie Funk: I would highlight the network of experts that I engage with around the world, especially civil society groups and activists in the [global majority](#). That’s where I spend most of my time: building relationships with and listening to people who are on the frontlines of these trends, and then thinking through how I can use my position as somebody living in the US to raise awareness about these challenges. I also try to engage with people actually building technology, who help me learn what issues can or can’t be solved with technical solutions.

Q: Last question: What advice would you give to someone wanting to do what you do?

Allie Funk: I would give three [pieces of advice] that I think are really, really important.

The first is relationships. Be kind to people, follow up with them — especially when there isn’t a tangible opportunity in front of you. So much of where I have ended up is because of a random relationship with someone I met at an event years ago.

The second is to be really open to opportunity and not too rigid. My career has been extremely serendipitous and nonlinear. I’ve tried to focus on what skills I want to gain, what issues I want to learn about, and what relationships I want to build, and just embrace opportunity when it comes.

The third piece of advice is also the most important: protect yourself and prioritize work-life balance. It took me time to realize that operating at 100-plus percent did not mean I was doing better work. It just meant I was burned out and I couldn't give myself what I needed. So really keep in mind the work will always be there. You're never going to finish the to-do list. Instead, you need to take that time away

because that's actually what's going to make you more effective in your job.

About

The Tow Center for Digital Journalism, established in 2010, provides journalists with the skills and knowledge to lead the future of digital journalism and serves as a research and development center for the profession as a whole. Operating as an institute within Columbia University's Graduate School of Journalism, the Tow Center is poised to take advantage of a unique combination of factors to foster the development of digital journalism. Its New York location affords access to cutting-edge technologists, a strong culture of journalism and multiple journalism and communication schools, with outstanding universities attached to them. The Tow Center is where technology and journalism meet, and where education and practice meet.

