ironwall
by Incogni

Protecting journalists from the risks of personal data exposure

Executive Summary

Journalists today face escalating threats—including doxxing, harassment, physical intimidation, and targeted cyberattacks like phishing and ransomware. These risks extend beyond individuals to the organizations they represent, creating serious vulnerabilities for print, broadcast, and digital media outlets. From account breaches and reputational damage to legal and financial consequences, the cost of inaction is high.

At the core of these threats is one critical weak point: exposed personally identifiable information (PII). For over a decade, Ironwall by Incogni has provided industry-leading online privacy protection by detecting and removing sensitive personal data, such as home addresses, phone numbers, and family details, from anywhere a search engine can find.

Our enhanced protection tools not only remove existing PII but also prevent new information from being sold, shared, or republished online. We help safeguard journalists, support staff, and organizations and provide long-term protection to reduce the risk of future targeting or attacks.

Protecting the privacy and security of journalists

It is the calling of a journalist to cover news stories, but in recent years too many journalists have become the focus of stories about threats, intimidation, attacks, persecution, online harassment, and even murder.

According to UNESCO, a journalist has been killed an average of every four days over the past decade.[1] Most of these incidents did not occur among foreign correspondents in combat zones, where the danger is obviously greater. The UNESCO report cited “political leaders, extremist networks and partisan media as some of the biggest instigators and amplifiers of online violence,” particularly against women journalists. The UNESCO report found that 73 per cent of women journalists surveyed said they had been threatened, intimidated and insulted online in connection with their work.[2]

The loss of public trust in the media is another contributing factor. Polls on this issue ebb and flow, but attacks against journalists increased during controversial coverage of the COVID pandemic and have yet to subside. A February 2025 Gallup survey found that American trust in the media dropped to its lowest point in five decades.[3]

"There was a hope at the beginning of the Biden administration that things would get better for journalists. And what we've seen, actually, is that things haven't really gotten better. They've stayed the same or worsened in some situations," Katherine Jacobsen, CPJ's U.S., Canada and Caribbean program coordinator, told Voice of America.[4]

The numbers paint a concerning picture. As of September 2024, **assaults on journalists in the United States in relation to their work have risen by more than 50% compared to last year** — from 45 to 68 assaults — according to data from the U.S. Press Freedom Tracker.

The fast and easy accessibility to personally identifiable information (PII), such as home addresses, cell phone numbers and other sensitive data, increases the danger for journalists, especially those reporting on the very communities they live in.

Every reporter is one controversial story away from becoming a target. That risk was illustrated in 2022 when Las Vegas Review-Journal reporter Jeff German was stabbed to death outside his home. German had written a story about corruption in the office of Clark County public administrator Robert Telles, who was convicted of German's murder.

How we got here

In 1962, MIT computer scientist J.C.R. Licklider envisioned a "Galactic Network" of globally interconnected computers through which everyone could quickly access data and programs from any site. It would take another three decades for that concept to mature into what we now know as the internet.

Like many visionaries, however, Licklider could not foresee all the ways the technology in his prophecy could be misused. Just as the inventors of the automobile also invented drunk driving, the men and women who developed the internet may not have anticipated how the instant availability of information – about anyone, anywhere, delivered with a handful of keystrokes, could be dangerous – even life-threatening.

As internet access and usage became pervasive, millions of Americans were eager to take advantage of its many conveniences – shopping online; paying bills online; downloading apps to save money on groceries, or to make a reservation at a restaurant.
The internet didn't ask for much in return – only a few personal details to register for an account: your home address, your phone number, your email address, and your date of birth.

Perhaps the entities collecting these personal details only wanted to provide better service. But as they built a database of names and addresses, they realized that if they also had the names and as they built a database of names and addresses, they realized that if they also had the names and addresses of other people, they could market their products or services to them. Lists were sold or exchanged, and data brokers began appearing online, offering home addresses and other once private information to anyone willing to pay for them – no questions asked.

As of 2024, there are more than 5,000 data broker companies worldwide, constantly collecting personal information from more than 1,400 leading brands. These brokers use secret algorithms to unknowingly build profiles on every American. The global data broker service market is expected to reach $407.5 billion by 2028.[5]

Information is power

All of us, to varying extents, have sacrificed some of our privacy for the convenience of online communication and activity, and we understand that many of the records once stored only on paper are now accessed electronically. As a result, however, anyone can now search for an individual online and find out where they live, the name of his or her spouse and where they work, and where their children attend school.

All an aggrieved party needs is the name in a reporter's byline to get their address. Enter it into Google Maps and look – there's the reporter's house or apartment building. Switch it to an aerial view and look at all those places for someone to hide outside. And with a couple more clicks they can find out where their kids go to school.

The widespread availability of personal information online has significantly contributed to the rise of home-based threats and intimidation campaigns. Those seeking to target journalists understand the psychological impact of shifting the threat from the workplace to the home.

Anger + Information = Danger

While it would be unfair to "blame the victim" when a journalist is threatened or attacked, the internet has also birthed a profusion of new media sources across the sociopolitical spectrum, most of which make no claim to fairness or objectivity.

Sensationist "click bait" headlines, coupled with the widening of political divisiveness and a decline in empathy has created a more dangerous culture where personal attacks and demonization over a single story or allegation are now commonplace.

And it's not just journalists and other public servants anymore – it's physicians, attorneys, airline ticket agents, small business owners, restaurant servers, and many others whose professions may incite an angry client. More than two-thirds of Americans had either been doxxed themselves (21%) or personally knew someone who had (62%).

What's more troubling is that these attacks often stem from misinterpreted statements, misinformation, or false accusations. But whether the trigger is real or imagined, the result is the same: an individual's narrative shared online can rapidly incite widespread outrage and condemnation.

It can happen to anyone at any time. Angry people can easily find anyone in both the digital and physical worlds, accessing their home address through hundreds of online sources.

Artificial intelligence's growing threat

Companies have always collected information to improve sales. The internet and our willingness to trade privacy for online convenience have significantly eased this process.

But today, organizations are not just collecting information to sell more products. They are collecting information on our opinions and behavior – where we go every day and what we do, what makes us happy and what makes us angry, and leveraging that data to generate an emotional response – and more views and clicks.

A recent global investigation by more than a dozen media organizations found that Pegasus spyware had been used to spy on journalists, as well as business executives and human rights activists. Pegasus software is a malware that infects both iPhones and Android devices and grants access to all information stored in a smartphone. It can also secretly activate microphones.

More than 50,000 cell phone numbers were obtained, among them those of journalists at some of the world's largest news organizations, including CNN, the Associated Press, Voice of America, the *New York Times*, the *Wall Street Journal*, *Bloomberg, Le Monde,* the *Financial Times* and Al Jazeera.

Addressing this challenge

The objective now must be to provide security services that reach beyond the workplace and into the homes of those who report the news, and to do so within constrained budgets. This raises a critical question for newspapers, digital outlets, and local broadcasters: **How should they respond when their journalists face threats not just on the job, but at home?**

Three options are available

Option one: doing nothing

Like car insurance, online privacy protection is something you invest in before something goes wrong. And while car accidents haven't become more frequent for most drivers, the number of targeted threats against journalists continues to climb. The internet now offers a wide array of tools to anyone intent on retaliating against a reporter over a story they perceive as unfair.

Social media offers an outlet to share grievances on platforms with millions of subscribers. "Fake News Covers Up Facts" and "Trump-Hating Journalist Lies About Immigration Policy" are the types of posts that many would click on, unaware that they are reading only one account of these situations.

These posts inevitably generate similarly outraged responses and may escalate into death threats against their source. As the online words get sharper, people react more viscerally and may eventually carry out violent actions in the real world.

It's easy to view inaction as the most economical option available. However, there are additional costs associated with privacy issues that are often not acknowledged. Journalists that receive threats and do not feel protected by their employers are more likely to have morale issues, take more frequent sick and vacation days, and perhaps even opt for resignation or early retirement.

Going it alone

Journalists could, in the absence of any help from their employer, take action to provide privacy protection for themselves and their families. This would require frequent online searches to locate where their private information is available, and emails demanding that this content be removed. However, doing so is a long, arduous, and time-consuming process that at best will yield imperfect results.

When information is removed, many state statutes require that it only stays removed for a limited period. It may also be reinstated by mistake (Bob Jones has his address removed, but Bob D. Jones [same person] is still listed on a website). Many sites that profit from selling information will simply ignore requests to remove it, knowing that they risk a punitive fine, but that risk is likely minimal.

Should an individual be successful in his or her efforts, that success will be temporary without constant monitoring. Buying or refinancing a home, getting a credit card, getting married or divorced, opening a bank account, or even signing up for a loyalty program at a grocery store can result in new information entering databases. And then the removal process starts all over again.

Given the time and effort necessary to find this content, remove it, and make sure it stays removed, more journalism organizations are contracting with outside agents that search, remove and, in a few cases, sue repeat offenders.

Option two: online privacy protection

Given the ever-escalating rise in threats and attacks, it is almost inevitable that every print, online and broadcast media provider in every state must one day contend with situations where someone fears for his or her safety.

When this happens the company must assume some responsibility for that person's protection, which should also extend to family members. That may entail a wide range of expenditures, up to and including security personnel, professional consultation on threat assessment, and other emergency measures. All these efforts, none of which had been calculated in the company's annual budget, will be far more expensive than investment in the type of advance precautions that contribute to a secure and sustainable workplace.

Option three: provide protection after an attack or credible threat

Many programs on the market claim to offer online privacy protection, but their services are often limited. Most simply monitor common people-search sites and either send automated takedown requests or notify clients when their information appears—leaving the actual removal process in the hands of the individual.

For some in the public this may be sufficient. It will lower participants' exposure and may keep them away from a few online scams and annoying robocalls. Such programs, which have proliferated over the past few years, also allow employers to assure their personnel that something has been done to make them feel more secure.

But limited searches of private databases and one-time removals are insufficient to address the nature and seriousness of threats against journalists. Companies that pay lip service to protecting clients, while not actually doing it, are putting those clients and their families in danger.

Some are at least honest about it – they say they'll check only those few sites where private information is most likely to turn up. More robust services seek out and remove sites on social media, county assessors, and malicious private sites, which are relatively common when someone has a grievance. However, these are generally prophylactic measures and work best before someone is threatened.

Comprehensive privacy protection programs are available, and are now being utilized by a wide range of public and private sector organizations, from courts and law enforcement agencies to healthcare and financial services providers. These programs are made up of several components that work together to remove private data from the internet, reduce the chances of it resurfacing, and equip members with additional tools to enhance their safety.

Some of these companies search only data brokers and people-finder websites for client PIII Ironwall by Incogni uses proprietary software to conduct searches across every aspect of the internet, not just a few select sites. When a client's home address is located, a series of communications is initiated with that website until the content is removed. Those that do not comply are referred to the state attorney general or taken to court.

Education is another key factor. This may be offered through training classes and webinars that increase awareness and provide a greater sense of confidence in personal security.

When compared to the cost of physical security and heightened protection after a breach of information occurs, or an attack at a home, these preventative measures are cost effective.

The Ironwall by Incogni Approach

There is a reason why thousands of individuals from all walks of life trust Ironwall by Incogni to keep them safe.

First, as previously stated, **we monitor all aspects of the internet – not just a few select sites.** Your name and address may appear on thousands of websites, not just those that specialize in "people finder" services. We track them all. When we find content that shouldn't be there, we don't just let our client know and expect them to do something about it – we take direct action to make sure that content is removed. **Our approach is so thorough that we remove 1.5 million pieces of private information every week for our clients.**

We cover our clients' household family members as well, because someone determined to go after a person they have targeted will also try to locate them through the online profiles of spouses and children.

In addition, we take a more strategic approach to privacy protection that is not limited to data removal. Since we can't stop thousands of companies from collecting and sharing information, we provide solutions for clients that replace authentic identifying content with content that cannot be traced back to the user.

VPN

One of the most effective ways to protect browsing and search activity online is to secure all logins, passwords and private information by adding a VPN to phones, computers, and tablets. A virtual private network (VPN) encrypts and safeguards all information submitted through WiFi and anywhere on the Internet. That stops anyone from looking at what you do online and sharing or monetizing that data.

A VoIP number

Most people rarely change their cell phone numbers, which is why these numbers are highly prized by marketers. It's also why you should never give it out to any company. However, certain organizations (especially banks) may demand that you provide a mobile phone number. When that happens a VoIP number can be provided that is different from your cell number, so it cannot be used to track you. Calls are then automatically forwarded from that number to your actual cell phone number.

You can also forward SMS messages (used for two-factor authentication), and let callers leave a voicemail that gets sent to your email as a recording. Our VoIP numbers are registered to us, and that is all anyone who contacts us will find out. We will never share or sell any of your information.

Email aliases

People share their email address with friends and family – but also likely share it with pizza delivery places, stores, restaurants, online retailers, and hundreds of other entities who will share or sell that data, increasing the risk of scams and identity theft.

Ironwall provides clients with secure alternate email addresses, to use in place of a personal email address. These alias emails all forward automatically to your actual email address, without revealing it. Services such as Gmail and Outlook also provide disposable email addresses, but Google can use those systems to track you. With Ironwall, your private information will never be shared or sold.

can use those systems to track you. With Ironwall, your private information will never be shared or sold.

Because databases are updated all the time, it won't be long before data brokers and scammers will not be able to build an accurate profile on an individual if that person's email and cell phone number do not trace back to the actual person, as their real identifying content is taken out of circulation.

Dark web monitoring

We monitor leaked email accounts and passwords online, looking for breaches and notifying clients if they have been exposed, putting their online accounts and financial information at risk. We can't remove it from the dark web, but we can make the information contained there less useful and less dangerous.

Emergency protection

If the worst happens — your personnel are threatened online, targeted or doxed — Ironwall responds with emergency support. We track the attackers online, monitor escalation patterns, violent threats, and suspicious behavior, and report back to your organization or to law enforcement. We conduct more extensive searches and extend protection to others in your executive's extended families, whether they reside with them or not. Our emergency support has been praised by law enforcement for saving lives and preventing tragedies.

Now is the time to protect journalists

Personal information is the foundation for every threat, every phishing attack, and every attempted identity theft. That is why it is essential for journalists – and the companies that employ them - to take control of their information, and limit access before it can be weaponized.

With new laws, growing public awareness, and increased funding for non-traditional threat prevention, there are more tools available today than at any point in the last 20 years. Privacy protection has evolved into a service that can be deployed quickly and affordably, and for a modest investment, journalists and newsrooms can shift this burden to professionals who specialize in data removal and threat prevention.

But not all privacy solutions are equal. Most offer surface-level monitoring or automated takedown requests that leave journalists exposed. This work cannot be done halfway—and it shouldn't be. For those who hold power to account, **the consequences of inaction are real, and sometimes irreversible.**

Start protecting your journalists today

Let Ironwall by Incogni help eliminate online vulnerabilities before they turn into threats.

Request a quote

Visit **ironwall.com** to learn more about how we can protect your team.

Request a quote

[1] https://courier.unesco.org/en/articles/journalism-dangerous-profession

[2] https://www.unesco.org/en/threats-freedom-press-violence-disinformation-censorship

[3] https://thehill.com/homenews/media/5167582-trust-media-record-low-gallup/

[4] https://www.voanews.com/a/us-press-freedom-under-unprecedented-pressure-report-finds/7806682.html

[5] https://techjury.net/blog/data-broker-statistics/#:~:text=%0D