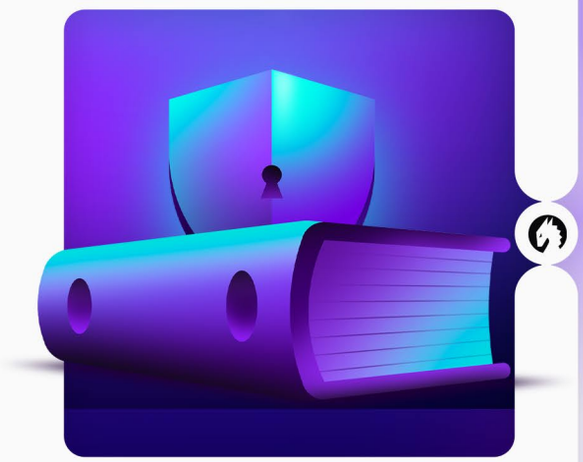
ironwall
by Incogni

What police departments & organizations need to know about online security



Introduction

Police officers are safer than they were 50 years ago. That's the good news. But while investments in new procedures and technology have been effective in protecting officers while on patrol, these measures can do nothing to protect them – and their families – after the end of their shifts.

Imagine you're a police officer, and you make an arrest, and the daughter of the man you arrested believes you were wrong, or used excessive force. So she tweets a link to a webpage that lists your home address, and the addresses of your relatives.

No need to imagine – it already happened in New York. And that tweet was viewed by thousands of people, and re-tweeted nearly 500 times.

Such methods of retribution are no longer rare. "Doxing" – the act of publicly revealing previously private personal information about an individual or organization through the internet, is now a common occurrence.

- In Los Angeles, an unknown individual posted the names and addresses of two officers online, as well as information about their children's schools
- More than 100 police officers in L.A. County had their addresses, names and phone numbers published
- 38 law enforcement officers in Portland, Oregon, were doxed amid ongoing protests in the area
- Chicago Police officers became the targets of doxing attacks, in which their personal information was shared on social media

In situations like these, targeting a private residence also puts a police officer's family at increased risk.

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. This content is gladly sold by "people finder" websites with no regard for how it may be used. The ubiquity of personal information on the Internet has had a profound impact on the escalation of home-based threats and intimidation campaigns. Groups that wish to target law enforcement personnel understand the psychological effects of taking the fight from the station house to the home.

Statute-Based Protection

At present there are 24 states that provide some level of online privacy protection to public officials. In addition, most states are currently considering consumer privacy legislation that would allow anyone to "opt-out" of having his or her personal data collected, shared, or sold. However, laws are just words on paper unless they are enforced.

Addressing This Challenge

The objective now must be to provide security services that reach beyond the officer's department and into their homes, and even into cyberspace, and to do so within tighter budgets. How should law enforcement organizations respond when their personnel are endangered outside the workplace?

Three options are available:

Option One: Doing Nothing

Like fire insurance on a home, online privacy protection is an investment against an occurrence that may never happen. However, while the number of residential fires has not risen over the past decade, one cannot say the same about the number of threats and attacks against police. The Internet now presents a cornucopia of options to the individual determined to seek vengeance against an arrest or a speeding ticket that is deemed unfair.

Social media offers an outlet to share grievances on platforms with millions of subscribers. "I Was Only Arrested Because Of My Race" and "Why Our Police are No Better Than Nazis" are the types of posts that many would click on, unaware that they are reading only one account of these situations. Such posts may be picked up by blogs, local media, or cable news channels, further increasing their reach. These posts inevitably generate sympathetic responses, and may escalate into death threats against the officer is who invariably named in the post. As online words get sharper, people react more viscerally, and may eventually carry out violent actions in the real world.

There have also been situations where offenders have created websites specifically to target an officer, often using his or her name in the URL. The reach of such sites is comparatively limited, but they may be indexed by search engines and appear if someone searches for that person. And once someone with a grudge has an officer's home address, any number of disturbing scenarios may result.

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.

The numbers are staggering:

- Seattle – As of 2024, has lost more than 700 officers in the past four years
- Minneapolis – Down more than 800 officers since the pandemic
- Baltimore – Down more than 600 officers
- Cleveland – More than 300 openings that need to be filled

Police who receive threats and do not feel protected by their department are more likely to have morale issues, take more frequent sick and vacation days, and perhaps even opt for resignation or early retirement. Over the last two years, police officers have been retiring early or just flat quitting in droves.

According to the Police Executive Research Forum, from 2019 to 2021 resignations for officers are up 43%, and retirements are up 24%. As a result, police departments across the country are dealing with crippling personnel shortages.

Law enforcement personnel 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 (Officer 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 the officer 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, many courts are contracting with outside agents that search, remove and, in a few cases, sue repeat offenders.

Option Two: Provide Protection After an Attack or Credible Threat

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

When this happens the department 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 of these efforts, none of which had been calculated in the department's annual budget, will be far more expensive than investment in the type of advanced precautions that contribute to a secure and sustainable workplace.

Option Three: Online Privacy Protection

Nominal programs exist that claim to provide online privacy protection. Such programs monitor the sites where private content is most likely to turn up, and then send a form letter requesting its removal, or report search results to their clients and have them follow up directly.

For some in the general 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 police organizations 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 police and other professionals who make life-and-death decisions every day. Companies that pay lip service to protecting clients, while not doing it, are putting those clients and their families in danger. Comprehensive privacy protection programs are also available, and are now being utilized by Supreme Court justices, federal justices, police organizations, and government agencies.

These programs consist of multiple components that work in unison to eliminate the publication of the private data of subscribers, reduce the likelihood of such content being found at a later date, and equip members with additional tools to keep them safer.

Companies use proprietary software to conduct searches across every aspect of the Internet, not just a few select sites.

When an officer'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.

Since personal information is the foundation for the impetus of most threats, these companies also take action to control the dissemination of this information, and limit access to it when necessary, while simultaneously flooding channels with content that does not lead back to the people under protection. There are simple solutions for masking one's email address, cell phone number, and online search and browsing history.

Once these are implemented, the result is less genuine information to be exploited, and a replacement of identifying content with content that conceals the identity of the user, and thus cannot be utilized for nefarious means.

When such precautions are taken, the amount of information in circulation about an officer and his/her family drops by 30-50%.

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.

While cost is always a concern, a closer examination suggests that protecting the police at home can be more economical than protecting them at work. Costs can be shared on a state and federal level; states like Tennessee have introduced bills that provide protection and allocations of state grants to help pay for these services; additional law enforcement and judicial grants are available from the federal government.

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. For the average urban department (with 50 officers) the tab could be less than $20,000 a year.

Between changing laws and more allocation of dollars for non-traditional threats, there is more help available today for police officers than there has been in more than two decades.