Securing the Integrity of Our Judicial System:

Protecting Judges Beyond the Courthouse

Ron Zayas

Just 40 years ago, bailiffs were the only security provision in most American courthouses. That changed after the Oklahoma bombing, the 9/11 attacks, and a dramatic increase in threats against jurists.

Shoring up the physical security of the courthouse has met with notable success. In fact, 44% of judicial respondents to a recent Bureau of Justice Administration survey rated the security at their courthouse as "good to excellent."[1] While some will argue that hardened courts are an illusion (55% of state courts have no security personnel in court proceedings, and an astounding 26% had no screening stations for weapons), the overall impression is that security is much better.[2]

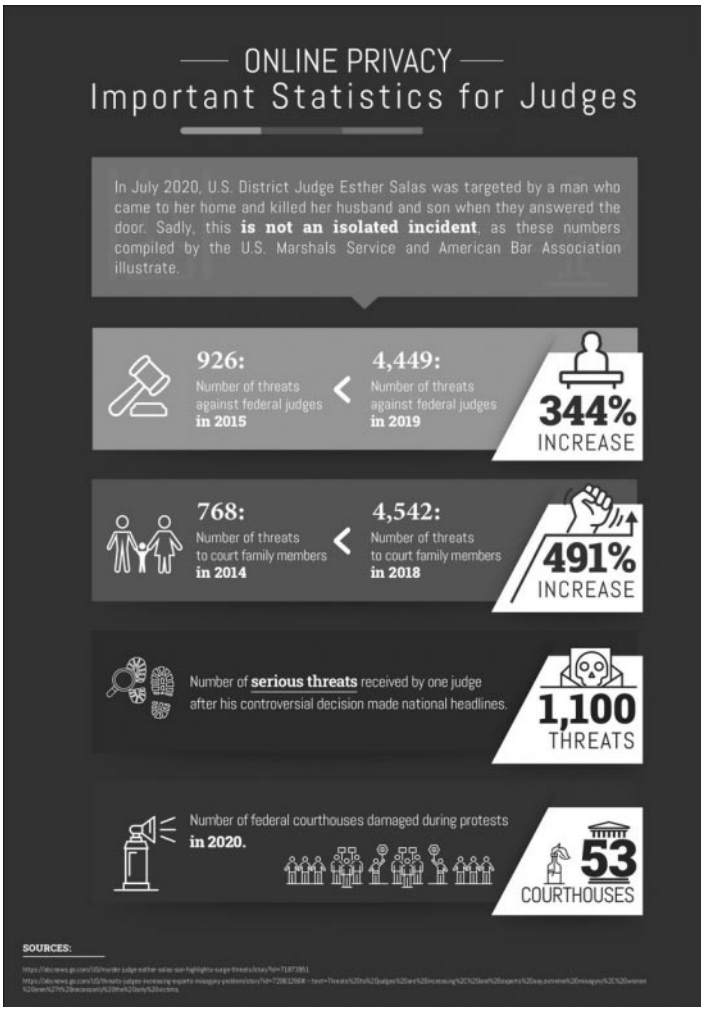
Despite these effective measures, threats to jurists continue and have evolved. Over the last four decades there have been 185 incidents of judicial shootings, arson occurrences, and bomb threats. And careful analysis reveals more than 400 additional incidents in the most recent seven-year window.[3]

During that same time, five federal judges have been killed. However, these attacks all occurred *outside* the courthouse, most frequently at the judges' homes.[4] The numbers are proportionately consistent with incidents in other areas of the state and local judiciary. Since then, threats against judges have increased and continue to be directed toward jurists in their home environments, paralleling the increase and nature of threats in society at large.

Forward-looking courts, administrators, and security personnel are eyeing beyond judicial facilities, and finding ways to make judges feel safer in their professions. That means providing security services that reach beyond the courthouse and into the homes of jurists, public-facing employees, and even into cyberspace. But as administrators face stiffening budgets, how and where to apply resources in the most effective way is always a concern.

Protecting jurists at home and away from the courthouse can be more cost-effective than protecting them at work. The reasons for this are varied:

- Because securing one's home is an investment in personal (not just judicial) security, the cost will likely be shared.



- Many attacks on the home of a judge originate in cyberspace; meaning the perpetrators gather most of their intelligence online, where preventing threats is also more cost-effective.
- Costs are more likely to be shared on a state and federal level, rendering them more affordable for individual courts.
- Due to the growing awareness of new threats, grants are

Footnotes

1. Timothy F. Fautsko et al., Status of Court Security in State Courts—A National Perspective iv, 5-2 (National Center for State Courts 2013), https://ncsc.contentdm.oclc.org/digital/collection/facilities/id/184.
2. *Id.* at iv.
3. *Id.*
4. Matt Reynolds, *An Attack on a Judge's Family Is Putting Judicial Security Center Stage*, ABA J. (Oct. 1, 2020, 11:25 AM CDT), https://www.abajournal.com/web/article/attack-on-judges-family-puts-judicial-security-center-stage#:~:text=Four%20federal%20judges%20have%20been%20murdered%20in%20the,of%20his%20Pelham%2C%20New%20York%2C%20home%20in%201988.

now offered at the state and federal levels to help jurists pay for protections or to give individual courts more discretion in how they implement safety programs tailored to their needs.[5]

THE EVOLVING THREAT TO JUDGES REQUIRES NEW APPROACHES

How did attacks move from the courthouse to the judge's house? While researchers point to different factors, these are the most frequently cited reasons for the change:

- Post-9/11 security protocols, designed to safeguard municipal facilities, are likely influential in would-be attackers looking to take the fight to less hardened sites. Increased focus on screening for weapons, greater visibility for deputies and bailiffs, including bomb-sniffing dogs, and increased video surveillance, means it is easier for assailants to be identified and caught during traditional attacks. New avenues had to be found.
- The planning involved in penetrating the typical courthouse's security measures increases the need for more co-conspirators, while elevating the chances of detection. Lone-wolf attacks are less likely to be successful in a secure building. While there has been an increase in mass shootings, the majority of these massacres have been directed at softer targets.
- Groups that wish to influence public opinion or protest the stances of individual jurists understand the psychological effects of taking the fight from the courthouse to the home. A court official accustomed to dealing with threats at work may feel more vulnerable when the attackers—violent or not—are standing outside their home and in proximity to their families.
- The proliferation of online attacks and the ubiquity of personal information on the Internet have really opened the door to threats. Simply put, anyone with Internet access can find the home address, family members, and relatives of a judge. Once the address is known, little more effort is required to then survey the property for areas of attack, identify the spouse and children of the judge, or even use phone data to track the movements of a specific judge. Arguably, the proliferation of this level of detail has enabled, if not driven, the move toward more personal attacks. In a common and related example of this type of attack vector, a blogger in California, upset at the legislature for passing gun control measures, published the names and home addresses of state legislators that voted for the measure. The blogger vowed to leave the information posted until the legislators changed their votes or died. Not surprisingly, the post triggered threats to the legislators, and in one incident to the son of a legislator who was home alone. The information was easily found on one of a hundred sites providing this content.[6]

Some courts, aiming to stay ahead of evolving threats, have worked with their judicial protection units to search for and identify online dangers and to provide information to judges through home vulnerability assessment and additional services when these risks arise. Many have found such options to be cost-effective. Members of the federal bench are protected by the U.S. Marshals office, but the Marshals have long stated that they lack the resources to protect judges from the escalating threats—many online—that are inundating courts and their protectors alike.[7]

SECURITY AS A GROWING EXPENSE

In the most recent budget request for the federal judiciary, court security accounts for $785 million, 11.5% more than the previous year, with growing threats against federal judges cited as a main reason for the increase.[8] Protecting the physical structures where judges work is imperative—and expensive—with billions more likely spent at the state, tribal, and county levels. In addition, the budget request specifically calls for IT infrastructure support at federal courts, citing the increased risk from foreign actors. But it also mentions the need for securing the **personal information** of judges. One of the witnesses, U.S. District Judge Roslynn R. Mauskopf, director of the Administrative Office of the U.S. Courts, said, "Our constitutional system depends on judges who can make decisions without fear of reprisal or retribution. This is essential not just for the safety of judges and their families, but also to protect our democracy."[9]

In addition to advocating for more funding for cybersecurity and the protection and removal of judges' personal information, Mauskopf specifically advocated for the passing of the Daniel Anderl Judicial Security and Privacy Act of 2021, which replicates statutes in eight states that make it illegal to post online the names and addresses of judges and law enforcement officials. The law is named after the son of Esther Salas, a federal judge who was targeted by an individual who found her home information online and attacked Salas's family at home, killing her son.

5. Associated Press, *Law Enforcement Encouraged to Apply for $100M Crime Grant*, U.S. NEWS (Oct. 12, 2022, 4:00 AM), https://www.usnews.com/news/best-states/tennessee/articles/2022-10-12/law-enforcement-encouraged-to-apply-for-100m-crime-grant; S. 2340, 117th Cong. (2021).
6. Eugene Volokh, *Restriction on Publishing Officials' Home Addresses Blocked on First Amendment Grounds*, WASH. POST.: The Volokh Conspiracy (Feb. 28, 2017, 2:55 PM CDT), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/28/restriction-on-publishing-officials-home-addresses-blocked-on-first-amendment-grounds.
7. Dan Mangan, *U.S. Marshals Service Lacks Resources to Protect Federal Judges Even as Threats Surge 81%, Report Says*, CNBC (Jun. 15, 2021, 2:25 PM EDT), https://www.cnbc.com/2021/06/16/us-marshals-lack-resources-to-protect-federal-judges-as-threats-surge-report-says.html.
8. U.S. Courts, Judges Request Funding to Address Cybersecurity, Courthouse Safety, Growing Workload, (May, 2022), https://www.uscourts.gov/news/2022/05/12/judges-request-funding-address-cybersecurity-courthouse-safety-growing-workload.
9. *Id.*

PRIVACY IS SECURITY

As noted above, the threat to our judicial system has evolved from full frontal attacks at the courthouse to more nuanced and possibly more effective attempts to change the hearts and minds of the judiciary and the public with attacks that are more personal in nature. Increases in these types of attacks have dovetailed with the availability of private information online.

Virtually anyone can search for an individual online and locate their home address, names of spouses and children, and even where family members work or go to school. Searches like these are so easy to conduct that they can often be completed in the heat of a moment, with no cooling time possible. Whether the information is found through a commercial "people finder" site that resells public information, through a malicious private site concerned with a specific individual, an agency or group looking to influence or hurt an official, or simply released through one of the daily breaches of collected data that happens in this country, the information is out there.

Countries that have stricter controls on how personal information is sold and gathered, such as those in the European Union, also tend to have fewer attacks on judges, but there can be other mitigating societal factors as well, such as gun control. Since the EU implemented its data protection policies—called GDPR—and enforced them against large data collectors like Google, the amount of personally identifiable information online has shrunk significantly. California implemented its own data protection system, often called GDPR-lite. While significantly less effective than GDPR and less rigorously enforced, it has also helped to lower the volume of online information for those who choose to exercise their newfound rights.

Privacy protection has come to the forefront because many of the attacks on judges have originated in recent years from information found online. Some states, and most recently the federal government, have either passed or introduced bills for statutes that move judges and law enforcement individuals into protected classes in terms of personally identifiable information that can be shown on websites.

STATUTE-BASED PRIVACY

Understanding the extent of private information that can be found online is staggering. A simple search for an individual appears below.

This search is typical of what you will find with data brokers, and includes relatives, addresses, phone numbers, and known emails. This information is refreshed on a regular basis and is compiled from public records, as well as from other sources such as credit reports, loyalty clubs, "free" services, social media, and even phone and internet providers.

Statutes in eight states (California, Texas, Nevada, Idaho, Utah, Colorado, Florida, and New Jersey), along with bills pending in at least six other states, and the federal Daniel's Law (named after Federal Judge Esther Salas, mentioned *supra*), aim to suppress this information. A judge or other protected individual could request/demand that their information be removed from appearing in these databases, or generally in any online source of information. When the information is removed, many state statutes require that it stays removed for a period of time. However, the information tends to come back regularly due to

Figure 1 — People Search result

mistakes (for example, "John Smith" being removed and "John R. Smith" being added), and to the general unwillingness of many providers to be thorough. Several state statutes allow for punitive fines to be assessed, but the onus is on the individual to take that initiative. Few do.

Refinancing a residence, getting a new credit card, getting married or divorced, or selling/buying a home can flood these databases with new information. Because of the time and effort involved to monitor and remove any content in violation of privacy laws, many courts are turning this responsibility over to outside agents that search, remove and, in a few cases, sue repeat offenders. Commercial database brokers, and even malicious actors, tend to respond to financial penalties and levies more than to legal requirements that are not enforced, making a lawsuit, or the threat of multiple lawsuits, more effective than multiple requests. In some states, the attorney general can also get involved when he or she is notified of egregious behavior and is presented with a clear, detailed evidence trail of misconduct. There are privacy protection companies—although very few—that provide this service and will even sue on behalf of their clients.

While some providers only search paid "people-finder" type sites such as Spokeo and BeenVerified, 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 with a judge. Of course, these are generally prophylactic measures, and work best *before* a judge is threatened.

PREVENTING PRIVATE INFORMATION FROM BEING AVAILABLE

In addition to the active searching and removal of information, some privacy protection companies provide clients with the tools and training to prevent the release of their information, and the ability to change existing information. White-glove, comprehensive services will usually provide—in addition to hands-free removal services—a VPN, email aliases, a VoIP number, and even mail forwarding that breaks the chain of causation between public information and the underlying recipient (i.e., the protected judge).

Tools like these, when set up and managed correctly, can replace content already available on the Internet with new,

untraceable information. More importantly, it allows protected individuals to resume mostly normal lives and enjoy the advantages of things like loyalty clubs, ordering a pizza, or using two-factor authentication, without compromising the safety of their families or themselves.

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 court (with 50 judges) the tab could be less than $20,000 a year. Many states, including Tennessee,[10] have introduced bills that provide protection and allocations of state grants to help pay for the protection. The federal government has also included law enforcement and judicial grants that can be used for protection services.

THE ROLE OF PRIVACY STATUTES

Good privacy statutes are the foundation for protecting judges. With these statutes being the "minority rule" among states, advocating for a statute if your state does not have one, or lobbying your congressperson to include all judges in the federal law at both the court and individual level, is an optimal way to establish protective statutes. Removing personal information without a state statute can be achieved to a more limited extent but is still possible.

PHYSICAL PROTECTION OUTSIDE THE COURTHOUSE

In addition to protecting the private information of judges, some courts are becoming more active and limber in evolving their definition of judicial protection. According to Bob Fleshman, the CEO of Napa County Superior Court in Northern California, this evolution includes a wider range of threats that extend beyond the courthouse. In addition to protecting the privacy of his judges, he has dealt with COVID-19, an outbreak of Legionnaires' Disease that spread to the courthouse from a nearby hotel, and with destructive fires. His efforts have evolved into a 360° approach to security and safety, something more and more courts are adopting on a daily basis.

Peter Ada, judicial protection expert for Orange County Superior Court (OCSC) in Southern California, is part of a team that provides leading edge protection to its judges. As a component to OCSC's comprehensive view on security, Ada will often work with judges outside the courthouse. Judges can partake in an assessment of their homes that includes a review of perimeter security, identifying areas that may be an issue, and protection upgrades. While the resulting safety costs are borne by the judges themselves, the expertise that Ada and his team bring to the table helps provide peace of mind.

As part of the vulnerability assessment, Ada will also conduct a comprehensive online profile of the judge and his or her spouse and will discuss any other concerns the judge may have. If there are any specific concerns, Ada and his team find that an effective Threat Assessment and Management strategy often helps deescalate a situation. His approach has met with great success and has provided the judges he serves with an overall increased sense of protection. OCSC is also one of a small but growing number of courts with an Emergency Response and Security Services Manager, a position dedicated to marshaling resources for judges and other court personnel. While not every court has the resources necessary to handle all threats, courts like OCSC and Napa are finding innovative ways to prevent incidents and, like most proactive measures, find prevention to be generally less costly than remediation later. Even so, Ada feels that having a dedicated budget for helping judges secure their homes would be an effective and efficient improvement to his services.

Protection has also been expanding to include court executives and any employees who are public facing. In today's societies, even innocuous threats can escalate into issues. Mediators, attorneys, bailiffs, and clerks can find themselves at the receiving end of a vendetta from someone who lost a case, or just does not feel that they were treated the way they deserved.

TYPES OF THREAT VECTORS

Sharing details of specific threats is always a sensitive subject that few want to go on the record about, as doing so could encourage more attacks. But a survey of threats outside the courts, encountered by my company, which has been helping courts protect judges for more than a decade, typically fall into the following categories.[11]

Social Media and Website Attacks. While anyone who is unhappy with the outcome of a trial, injunction, or judicial order can become a threat, a survey of threat vectors shows that decisions (and the people involved in making or enforcing the decisions) in family law, civil trials, and criminal courts have the highest incidents of escalated issues outside the courtroom. It is not surprising that family law, with its ability to render decisions that affect marriages, children, and homes, would have an elevated propensity for escalated threats. Family law issues account for over 45% of all incidents that bleed outside the courthouse or play out online.

Offenders in this area have been known to use social media to recruit sympathetic supporters who may only be seeing one side of the story but are often pulled in with heart-wrenching headlines ("Callous Judge Sent My Daughter to a Child Molester" or "My Husband Abused Me and My Children for Years and the Judge Gave Him Custody"). Without a complete picture of the situation, stories like these become clickbate on social media and are shared often and far-afield. Well-meaning people—heartbroken over the pain felt by the poster—begin to offer advice, which can start as a recall campaign, and quickly escalate into a death threat. A sympathetic blog will generate posts and comments, often anonymous, and such comments feed on each other. Trolls, or even just borderline individuals, will use strong words to react to a situation, and another poster will take it a step further. This online disinhibition effect provokes people

10. Corinne Murdock, *Proposed Bill to Protect Law Enforcement, Judges from Civil Rights Intimidation*, Tenn. Star (Feb. 20, 2021), https://tennesseestar.com/2021/02/20/proposed-bill-to-protect-law-enforcement-judges-from-civil-rights-intimidation.

11. Internal review of types of flagged incidents reported, 360Civic/IronWall360, covering more than one million points of data since 2015.

to behave online in ways that they would not normally in real life situations.[12] As the online words get sharper, people react more viscerally, and may eventually carry out violent actions in the real world.

Watching these types of interactions develop and grow is an important aspect of seeking out potential threats and neutralizing them before they lead to actual encounters.

In addition to social media posts, offenders can create websites that often have the target of their attacks in the URL (e.g., JohnSmithJudge.com). Although usually crude, these sites—linked and promoted on social media—can draw a great deal of sympathy and come up prominently when searches for the specific judge or individual are made. While they may not explode in popularity or become viral, they can be very disconcerting to the individual targeted, who is more likely to search or notice search engine results under his name. These types of websites can range from First Amendment annoyances that impugn the credibility of the victim, to sites that provide specific roadmaps of how a "corrupt" official should be punished. Being aware of these types of sites and learning how to distinguish the nature of the threat is critical to providing protection.

Coordinated Online Nuances. Sometimes the goal is not to attack someone but to annoy them or cause them economic distress. Knowing the personal email, social media page, home address, or names of family members allows motivated individuals to wreak havoc. In 17% of threats we cover, someone provides an email for questionable sites, exposing the victim to phishing scams or having packages delivered. The modern equivalent of signing up people you disliked to magazine subscriptions, these types of attacks are usually intrusive but not dangerous. While it may be hard to protect targets (unless email aliases and other masking measures are in place), they rarely cause real-world injury, just some undue embarrassment. But their effect on the victim, making them feel vulnerable and helpless, can be significant.

Online/Offline Hybrid Incidents. In fully 13% of issues we surveyed, attack vectors involved a hybrid of offline and online issues. The best representation of this is when a disgruntled individual lists an open house at the residence of the victim, puts their car up for sale at a ridiculously attractive price, and uses the phone number of the victim as the number on the ad. Darker variations include signing up victims for dating apps or posting racist or sexist slurs under the person's name and email address.

Cyberattacks. The final category is one where the most destructive non-physical damage occurs. Cyber criminals can target judges specifically to gain access to their computers, as a pathway to access the networks and IT infrastructure of the court. Once inside they steal information or unleash ransomware strikes. While it is true that the identity of judges is public information, and that a judge's email is generally publicly known, courts also usually have more extensive protection and detection systems in place. Analogous to how physical attacks may have more success if perpetrated outside the hardened courthouse, so too are cyberattacks more effective if they can start at a judge's non-work devices and migrate to the court's infrastructure. These individuals typically do not have a concern or grievance with a particular judge but use this as a means to achieve financial or political goals by compromising the IT infrastructure of a court. But again, how they find out the private email, address, and other personally identifying information of a judge is related to online privacy issues and can likely be resolved by addressing those issues as discussed *supra*.

OTHER OFFSITE-ATTACK ISSUES

Not surprisingly, vectors of attack outside the courthouse are as varied as the imagination can allow. Whether it is some of the more common avenues discussed below or more creative options, most revolve around habits that can undermine the security of a judge and their family. However, as we will discuss in the solutions section, habits that put a judge in danger are among the easiest to rectify and change, with some education and reinforcement.

THE TRIP FROM WORK TO HOME

A danger point is always when a person can identify a consistent pattern for a potential victim. For most judges, the pattern that is generally most repetitive is the trip to and from work. Because it is easy to identify a judge with a particular courthouse, a motivated assailant can simply stake out the courthouse and look for the judge to leave. To do so, however, they must be able to identify the type of car the judge drives or have a keen line of sight on the drivers of all cars leaving the garage.

STARTING AT THE GARAGE

Many courts have secured their garages, looking for ways to make the ingress and egress safer for those with access. While locked gates and security codes are important, so is the training of judges to be aware of potential danger points (for example, waiting at the gate to leave while the guard arm is down) and the importance of situational awareness. In areas with longer commutes, it is easier for judges to be aware of cars that seem to be following them. While this can devolve into a paranoid obsession, basic training on driving techniques can go a long way to prevent a person from following a car and learning the home address of a jurist or court official.

THE DANGERS OF TECHNOLOGY

Of course, if you can identify the car of judge, or have physical access to it, a simple Apple tag or GPS tracking device can be used to gain valuable information on where the judge lives and any habits they have. These devices are generally small, easy to hide and, with magnets, can be installed in wheel wells or on the undercarriage of the car. Most can be found with a visual inspection of the car, and devices exist that make locating them simple. Some courts partner with law enforcement to make periodic

12. Social Media Victims Law Center, *Social Media Violence*, https://socialmediavictims.org/social-media-violence; Lauren Farrar, *Is the Internet Making You Meaner*, KQED.org (Aug. 5, 2019), https://www.kqed.org/education/532334/is-the-internet-making-you-meaner.

searches of cars to see if any trackers exist. While this danger is rare, it could become more commonplace as tracking devices get cheaper. Multiple sites on the web contain information on identifying and disposing of these trackers.[13]

It is also possible to gain access to some security gates and garage door openers by hacking the integrated garage door opener in your car (and using a programming unit) or stealing a removable garage door opener. Thus, someone gaining access to your car can possibly also have a way in. Integrated car door openers, if your car has one, are generally more secure, but if a person has access to certain technology, they can gain access. A removable unit is easier to steal, but also easier to hide or take with you. Also, invest in encrypted garage door openers that rotate the codes, since those are harder to spoof. In general, an encrypted, non-Wi-Fi enabled garage door opener is secure. Adding Wi-Fi and monitoring features, while convenient, increase the chance that it can be hacked.[14]

YOUR CAR REGISTRATION AND INSURANCE, PLEASE

It is common for many of us to keep our car registration and insurance in the glove compartment of our car in case we are pulled over or have an accident. Assailants know this, too, and a break into your car can easily provide information on where you live, along with the vehicles of your spouse and children. A more secure alternative is to keep a picture of your registration and insurance card on your phone, encrypting the photo, when possible, in case it is ever lost (see more on phone security later). Instructions for encrypting photos on an Apple or Android device can be found in the footnotes.[15]

YOU'VE GOT MAIL; DON'T OPEN IT

Once a person knows where a judge lives, it is possible to send them a malicious package. While again uncommon, it is not unheard of. Many courts have procedures for screening packages, but packages sent to homes and P.O. boxes will likely not be screened. Any parcel that is not expected should be treated with care and, if suspicious, a call for help from the local authorities may be prudent. Just as important is instructing young children and spouses on how to identify and be wary of packages that may be malicious in nature. Some judges are using a mail-forwarding service to screen their mail. In addition to protecting their home address, these services scan the front of a package or letter and allow the recipient to prescreen the package before gaining physical access to it. Also, since these addresses typically contain a telltale "Suite" or "Box X" second line, that tells a would-be attacker that a direct attack is unlikely to reach its intended victim.

The only issue to consider is that while P.O. boxes and mailboxes with private providers are popular and cost-effective ways to protect your mail, they are also commonly used to protect your address from being exposed. In this way, they tend to fail. The U.S. Postal Office requires that any mailbox have a notarized ownership certificate, with a valid ID and home address, whether you use one of their boxes or a commercial solution. A Freedom of Information Act request can easily reveal the owner of a P.O. box and their home address. Commercial services often sell the personal information of their clients, so if you get a mail-forwarding service be certain that is able to protect your identity completely.

PROTECTION ACROSS GENDER LINES

While men are more often victims of violent crimes than women,[16] women tend to have a heightened sense of the need for protection. One survey of who signs up for privacy protection among judges shows that 60% of adopters are female, when women account for only 49.7% of judges.[17] Courts may need to be sensitive to the special requirements and threats that female jurists face on the bench.

The amount of vectors for potential violence against the judiciary that happens outside the physical confines of the courthouse are myriad, but fortunately effective ways to address these threats are available and can be more economical than the cost of armed security at a courthouse.

TRAINING AND AWARENESS ARE KEY

In addition to protecting the privacy of judges to minimize potential dangers, it is also important to educate judges on the nature of attacks, both online and offline. These training solutions tend to increase awareness and provide a greater sense of confidence in personal security.

1. **Training classes and webinars.** A wide range of training avenues exist from private companies, law enforcement professionals, and even existing court vendors. Training is typically low-cost, helps identify holes in security, and helps members of a court work together. According to the Duke study cited previously, less than 25% of courts have a security committee that can look at security issues to identify and provide opportunities for training. Education is always an effective preventative strategy.
2. **Investing in privacy protection.** While covered extensively in this article, safeguarding the privacy of jurists is a vital part of any protection protocol. Advocating for protection statutes in states where they don't exist, teaching judges to understand how giving out informa-

13. Daniel Henry, *Does My Car Have a Tracker? How to Figure?*, AUTOCARNEED, https://www.autocarneed.com/does-my-car-have-a-tracker.
14. Michael Xavier, *Are Smart Garage Door Openers Safe? (Can They Be Hacked?!)*, GOOD HOME AUTOMATION (Aug. 20, 2021), https://goodhomeautomation.com/are-smart-garage-door-openers-safe.
15. Privacy Tips and Resources, 360Civic, https://360civic.com/privacy-tips-and-resources.
16. Statista Research Department, *Number of Violent Crime Victims in the United States from 2005 to 2021, by Gender*, STATISTA (Oct. 20, 2022), https://www.statista.com/statistics/423245/us-violent-crime-victims-by-gender.
17. Data on privacy protection statistics from 360Civic/IronWall360 participation among a sample of 2,000 judges sampled; percentage of female judges provided by Judge Demographics and Statistics in the U.S., Zippia.com (last updated Sept. 9,2022), https://www.zippia.com/judge-jobs/demographics.

tion impacts their personal and family safety, and partnering with companies that can remove information or train judges to remove it themselves is key to enhancing security. If an aggrieved person can't find the home of a judge or is delayed enough in the process to provide a cooling-down period, the chances of incidents decrease significantly.

3. **Partnering with law enforcement.** Whether it is a dedicated judicial protection unit, the sheriff's office, or the U.S. Marshals Service, these agencies can usually provide support beyond physical protection when a threat arises. Partnering with these resources, as some of the forward-thinking courts highlighted in this article have done, can lower the intensity and number of incidents. This is crucial, since law enforcement has been overwhelmed with the number of recent threats and the task of protecting 16,000 judges across the county.
4. **Understanding that threats affect the entire judicial system.** When judges feel threatened, they tend to experience increased sick days, health issues, and morale issues. They are less likely to run for reelection, and more likely to opt for early retirement. Issues with divorce or stress at home, caused by outside threats, affects productivity and compounds caseload problems. The hidden costs of not providing protection outside the courthouse can be costly in both the financial and physical sense. Without jurists who feel that they can make decisions sans fear of reprisals, our system of justice and government simply cannot work.

HELP IS OUT THERE

Court executives, administrators, and presiding judges can be overwhelmed by the escalation of threats against them and their peers, but awareness is slowing starting to catch up with the danger. Between changing laws and more allocation of dollars for non-traditional threats, there is more help available today than there has been in over two decades.

Ron Zayas is an online privacy expert, speaker, author, and CEO of 360Civic, a provider of online protection to law enforcement, judicial officers, and social workers. For more insight into online privacy laws, proactive strategies, and best online data practices, download a free how-to guide on protecting yourself at 360civic.com/privacy-resources. Connect with Ron at ron.z@360civic.com or LinkedIn.