

Tech and No-Tech Security Considerations for Judges

By Judge Herbert B. Dixon Jr. (Ret.)



Less than a week following the now-infamous January 6, 2021, Capitol insurrection, an article in the *Judicial Edge*, an online publication of the National Judicial College, asked whether the same sort of invasion could happen at courthouses across the country or even at the Supreme Court of the United States. Sadly, the article answered yes. However, the article’s author also offered several proactive undertakings to prevent or mitigate the damages. The author, retired U.S. marshal and judicial security expert John Muffler, suggested that the prevention and mitigation actions to prepare for such a catastrophe should include (1) establishing a court security committee that regularly meets to review and report on issues affecting security, (2) creating an encrypted information-sharing system regarding potential and current threat activity, (3) practicing “what-if” scenarios, and (4) engaging in continuity planning for catastrophic loss to the building and other facility infrastructure. Muffler emphasized that the persons responsible for court security must conscientiously accumulate actionable intelligence and have a threat management program at their disposal—having thought out what to do before, during, and after such an

event.¹ Not surprisingly, this discussion about institutional security preparedness caused me to wonder about individual security preparedness and the steps that individual judges might consider in contemplating their personal safety away from the courthouse.

Threats against judges do not occur only at the courthouse or in the nearby judges’ parking lot. Most often, they occur at locations more personal to the judge. For public figures, including judges, targeted planned attacks typically occur away from secured environments outside the courthouse, whereas impromptu emotional violence is more typical in a courtroom.²

While there are many instances of attacks on judges and other government officials that have contributed to the accumulation of knowledge about personal security, there is one tragic incident—an unsuccessful assassination attempt of Travis County Criminal Court Judge Julie Kocurek in Austin, Texas—that I find especially helpful for launching this discussion about personal security considerations for judges. The details of this attack are primarily taken from the transcript of a 2019 episode of CBS News’ *48 Hours*³ and a judicial security article by Muffler in *Police Chief Online*.⁴

On a Friday evening in November 2015, Judge Kocurek was returning home from a typical Friday night high school football game. Her teenage son, Wil, with his recently acquired learner’s permit, was driving. Judge Kocurek occupied the front passenger seat and visiting relatives were seated in the back. As Wil entered the driveway and prepared to activate the remote to open the security gate, he noticed a trash bag that blocked the car’s path to drive through the gate. Wil got out of the car to remove the trash bag when suddenly a gunman walked to the vehicle and shot four times through the front passenger window, wounding Judge Kocurek.

Judge Kocurek’s assailant, Chimene Onyeri, was subsequently arrested. He was tried and convicted following a month-long trial that included 840 government exhibits, 75 jail phone calls, 300 images, 33 undercover recordings, 36 videos, and dozens of witnesses that included the testimony of several associates. Onyeri was sentenced to life in prison for 17 offenses, including Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity that included a Special Sentencing Allegation of Attempted Capital Murder of Judge Kocurek.⁵ An after-the-fact analysis of this shooting identified several occurrences that form teaching elements for personal security specialists who consult and teach on the subject of judicial security.

Events Preceding the Assault on Judge Kocurek

Onyeri was a criminal defendant on Judge Kocurek’s docket, which included a motion to revoke probation based on the new offense. Onyeri was concerned about the consequences he may suffer before Judge Kocurek and started searching the internet for information about her. Within days of his court appearance, Onyeri located the judge’s home address, telephone number, and photos of the make, model, and license

plate of her cars. Afterward, Onyeri spent several weeks tracking Kocurek's patterns.⁶ He drove several times from his home in Houston to Austin to surveil Judge Kocurek and her family. Pictures on Onyeri's phone showed him driving so closely behind Judge Kocurek that one could clearly see the back of her head. At one point, Onyeri came to the windows of the judge's home to peek in.

Weeks before the assassination attempt, the district attorney's office received a call from Onyeri's girlfriend stating he was going to kill a judge in Austin. That information, which investigators deemed not credible, was not passed on to court security or judicial administrators. One night, Judge Kocurek noticed a jogger in street clothes go by her house; this curiosity, however, did not cause any concerns about safety or security.

The attack on Texas Judge Julie Kocurek paints a stark picture of the security challenges present around the home, even when judges take proper measures. The remotely operated security gate was a good security precaution; however, it was rendered ineffective by the trash bag placed in the driveway, which caused the car to stop before it could pass through the gate. As a result, the judge was a stationary target.

Awareness of Pre-incident Indicators

Security experts often label unique events that occur before an attack as pre-incident indicators (PINs)—in this case, the call from the girlfriend to the district attorney's office, the odd-looking jogger, the car following closely (driven by a person the judge might have recognized), and the trash bag blocking the gated entrance to the driveway. It is too simplistic to suggest that this tragic attack would have been avoided if all of these PINs had conveniently been wrapped in a package, tied with a bow, and delivered to security experts in advance of the attack on Judge Kocurek. However, as a part of their typical review of events leading up to an attack, judicial security experts will ask whether the attack might have been averted if the threat to kill had been reported to court security officials and the judges, if Judge Kocurek had noticed the car following too closely or recognized

the driver, if neighbors had been warned to look out for people in the neighborhood they did not recognize, if there had been less information about the judge on the internet, and if the placement of the trash bag had been considered suspiciously odd. Although it is not possible to know if a different result was likely if the reaction to one or more of the PINs had been different, security experts point out instances where serious consequences were averted or lessened because of intuitive concerns about safety or a suspicion that something was not right. According to Muffler, the security expert who raised the question about whether attacks on courthouses as occurred at the U.S. Capitol are possible:

Loading one's security intuition can only be done when getting as much information as possible, credible or not. A law enforcement officer's development of reasonable suspicion and probable cause is much the same. Development of intuition and suspicion are based on life experiences and practices when the collective information is gathered and mentally processed in a reasonably objective way. What is out of place? Can I/should I act? Does a bag at a gate belong there on a non-trash pickup night? Am I aware of a threat to kill a judge? Without data, one is not fully informed to have heightened awareness and take necessary precautions.⁷

Thankfully, however, Judge Kocurek and her family survived this incident.

Measures Judges Can Take to Better Protect Themselves

Limit Public Availability of Personal and Family Information

Judges must take steps to protect themselves and their families outside the courthouse. They should be proactive in protecting their personal information. While not every suggestion among these considerations is mandatory, every occasion personal information is eliminated from public view is a protective buffer against prying eyes seeking to find,

confront, or interact with you inappropriately. Consider removing your personal information from all places where others might find it—from deeds to social media. On social media and other online interfaces, judges should opt out of providing personal information to the public and avoid making advance announcements of planned trips and events to be attended. Even comments on social media about trips or vacations in progress should be avoided as this advises the public that you are not at home. The admonition about removing personal identifying information not only applies to Social Security numbers, home address, names of family members, and dates of birth; it also applies to a license plate or other visible indication identifying you as a judge and bumper stickers that identify your children's schools.⁸

Be Aware, Especially in Familiar Surroundings

While it is a natural human instinct to be observant when a person is in an unfamiliar location, attacks on judges often occur at the judge's home or a place that is personally familiar to the judge other than the courthouse. For that reason, security experts recommend that judges should especially take note of their surroundings when arriving at those locations. Is something out of place; are there too many unknown people; does your intuition suggest that something is not right? Although



Judge Herbert B. Dixon Jr. retired from the Superior Court of the District of Columbia after 30 years of service. He is a former chair of

both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.



none of these occurrences or a combination of them is proof of something amiss, the experts suggest these are the times you should make an extra effort to be situationally aware.

Security Layers Around Your Home

John Muffler, the security expert cited previously, advises in the article *Protecting Your Castle: Residential Security for Judges* that judges should think of their home security in terms of concentric circles. Each circle, spreading outward from the family at home in the epicenter, provides an additional layer of protection.

Beginning with the outermost circle, the property's perimeter, there should be proper outdoor lighting and well-maintained landscaping allowing for good lines of sight. Motion-activated lights can be particularly effective, as they can act as an alarm when triggered, scaring away possible intruders. Motion-sensing devices should be placed out of reach so they are not easily tampered with. Lighting should be placed to evenly illuminate the property, reducing shadows and potential places to hide. When the interior of the home is lit, blinds and shades should be drawn, preventing a clear line of sight for an assailant.

Shrubbery should be kept trimmed to remove hiding places and keep the home visible from the street. Shrubs located near the house should be trimmed to three feet or less so they do not provide hiding places. Trees near the house should be kept at a

height that allows a line of sight from the home through the gap between the low-cut shrubs and the taller trees. While these measures may result in the loss of some privacy, they significantly increase security. Lighting can also be added to illuminate trees and shrubs to increase exterior visibility. Trestles on the home should not come near windows, as they can be used as ladders to gain entry. Sheds and storage areas need to be secured to prevent ladders or tools from being used to enter windows, to breach doors, or as possible weapons.

Doors, locks, and windows comprise the next layer of protection. Security experts suggest that exterior doors should be solid wood or metal; however, they recognize that esthetically, many homeowners will resist. Alternatively, the experts recommend exterior doors with as little glass as the homeowner is willing to accept. Deadbolt locks provide significant protection. Ideally, doors should be flush with the doorframe, and deadbolts should enter an inch into the frame. Locks that can be turned by hand from the inside should not be used on doors where a window can be broken, allowing the lock to be reached from the outside. Doors with these types of windows should be fitted with double cylinder deadbolts, which require a key to open the lock from inside.

Windows tend to be the most vulnerable part of the house. However, there are steps to minimize the vulnerability. Many modern windows have a laminate between

the two glass layers that requires multiple blows for the glass to shatter. This can deter intruders who wish to avoid making noise as they break in. Consider replacing your windows if you do not already have this type. Window pinning, where a nail or pin is placed in the frame of the sliding part of a window,⁹ provides extra security to prevent an intruder from opening the window from the outside.

Home security systems, including a video doorbell and other video surveillance, provide additional and critical layers of protection. In addition to video surveillance, your system should include alarm control panels in the lower level and primary bedroom, door and window contacts, glass break and motion detectors, and an alarm annunciator.

If available, a secure area within the home, or safe room, should be identified for use in the event of an intrusion, especially if exiting the home is not an option. The room should have a solid door with secure locks. Hopefully, your instincts and the pre-planning process will ensure that you grab your cell phone before making a hasty retreat to the safe room. Still, an added benefit would be to maintain a telephone in the room, especially a wireless phone in case the landline is cut. Isolating in the room can provide the time needed for help to arrive. If the room is on an upper floor and has an exterior window, install a rope ladder for use in the event a safe exit is possible.

While it is possible these concentric circles of protection will not ultimately stop an intruder, they place time and distance between the home occupant and the perpetrator, which can be critical. Along with these measures, judges should have frank discussions with their families regarding possible emergency scenarios and form an emergency action plan to respond to and evacuate from crisis situations.¹⁰ These scenarios include an established safe word, e.g., you are out in public with your family, and you say quietly to them, "Go call Aunt Susie." Through previous family discussions, because there is no "Aunt Susie," that is your silent and urgent advice to them that you perceive an uncomfortable situation or danger, and they must leave immediately *without debate or delay*.

Final Thoughts About Physical Security Consideration for Judges

Threat assessment is a complex task requiring specially trained investigators.¹¹ While security risks have always existed for judges and court personnel, threats against the judiciary have increased in recent years. The U.S. Marshals Service is charged with protecting approximately 2,700 federal judges and 30,300 other court officials at 866 court facilities. In the calendar years 2018–2020, the Marshals Service assessed an average of 4,417 annual threats against the judiciary, representing a 476 percent increase from 926 threats in 2015.¹² Unfortunately, similar information for threats against state judges is not readily available. Notwithstanding the absence of summary information regarding threats against state judges, if the federal trend is any indication that threats against the judiciary are on the rise, all judges would be well advised to become more proactive in their consideration of personal safety. And while you are at it, (1) check if your state or locality has enacted or is considering legislation

regarding the privacy of a judge's personal information and (2) consider whether adopting a dog would add to your security at home. ■

Judge Dixon wishes to thank James L. Anderson, Esq., Superior Court of D.C. senior judges' law clerk, for his assistance researching the topic of judicial security and preparing this article.

Endnotes

1. John Muffler, *The Left of Bang Principle*, JUD. EDGE (Jan. 11, 2021), <https://bit.ly/3fHJrHr>.
2. Madison Alder, *Shooting at U.S. Judge's Home Highlights Risks Outside Court*, BLOOMBERG L. (July 20, 2020), <https://bit.ly/3dLyUW>.
3. *48 Hours: Austin Judge Ambushed Outside Her Home Survives Attack with a Mission to Protect Others* (CBS News Aug. 31, 2019), <https://cbsn.ws/3wjD8gM>.
4. John F. Muffler, *Mitigating Targeted Violence in Our Communities: Learned Lessons from Past Attacks*, POLICE CHIEF ONLINE (June 3, 2020), <https://bit.ly/34whzj3>.
5. *Man Who Shot Judge Kocurek Sentenced to*

Life in Prison, KXAN (Oct. 2, 2018, updated Oct. 3, 2018), <https://bit.ly/3uG0ZaZ>.

6. Ryan Autullo, *Onyeri Sentenced to Life in Prison for Judge Kocurek Shooting*, STATESMAN NEWS NETWORK (Oct. 2, 2018), <https://bit.ly/3uDEJi2>.

7. John F. Muffler, *Judicial Independence: Threats and Security Considerations*, JUD. EDGE (Mar. 17, 2016), <https://bit.ly/3gGNNzd>.

8. *Judges Should Protect Their Security Online, at Home*, ABA NEWS (Nov. 9, 2020), <https://bit.ly/3eyzNFf>.

9. *Do Your Double-Hung Windows Provide an Easy Entry to Your Home?*, GOLD KEY SEC., <https://bit.ly/3fMBdOh>.

10. John F. Muffler, *Protecting Your Castle: Residential Security for Judges*, JUD. EDGE (Nov. 19, 2015), <https://bit.ly/3yU89M7>.

11. See ROBERT A. FEIN & BRYAN VOSSEKUIL, PROTECTIVE INTELLIGENCE AND THREAT ASSESSMENT INVESTIGATIONS: A GUIDE FOR STATE AND LOCAL LAW ENFORCEMENT OFFICIALS (Nat'l Inst. of Just. 2000), <https://bit.ly/2RZgRYP>.

12. CNN Editorial Rsch., *Judges Targeted Fast Facts*, CNN NEWS (Apr. 26, 2021), <https://cnn.it/3nhoxkm>.