Armed Citizens' Legal Defense Network, Inc.

Leveraging Tech for Better Personal Safety

An Interview with Felicia King

by Gila Hayes

Network members, have you considered the overlap of physical security with the technology that we use every day and take for granted? It's a concern that I struggle to understand, so, when a longtime member with whom I correspond occasionally reached out about leveraging internet technology to thwart known threats, she had my attention. For learners who enjoy video, see https://youtu.be/768_7FaYY9Q for a less tightly-edited version of my talk with IT security professional Felicia King.

eJournal: Members, I'm honored to introduce to you Felicia King. Felicia, could you tell us a little bit about yourself and about your work?

King: Thank you for having me. I am Felicia King from Quality Plus Consulting. We also are branded as QPC Security because security is mostly what we do. I've been doing this for about 30 years, and I'm not siloed exclusively in security. I do construction management; I'm a certified welder and I started working on engines when I was 10 years old. So, I'm a little different than most women.

I don't want people to think that the things I'm going to talk about are enterprise only. Because we've been in business for so long, a lot of our customers are retired individuals like retired secretaries or librarians. A lot of the things that I talk about and recommend are scalable from a retired person's budget all the way up to things that do work for business, as well. That breadth and depth comes from 30 years of consulting, construction management and living with the solutions that we implement. The long-term implications, supportability and total cost of ownership are very important in the things I recommend.

That is all pertinent to our discussion today because we want to enable people to be as self-sufficient and resilient as they can be, while finding good advisors to help them when needed.

eJournal: For those enjoying the video version of this interview, see the show notes for links to Quality Plus Consulting, to Felicia's podcast Breakfast Bytes (hint: it's not for IT professionals so check it out at https://www.qpcsecurity.com/category/blog/) and other recommended resources, too.

Online security is a challenge for those who don't work in the tech world, like me, so one thing I enjoy about knowing you, Felicia, is the emails that we exchange about personal security. That's our common ground and we've been talking about these concerns for about 13 years now! In this series we will pick your brain about communications, surveillance, access control and even online safety. Let's call part one communications.

Part 1: Communications

eJournal: Felicia, you recently mentioned that you were leveraging your cell service to extend your coverage, and you're doubling up with Wi-Fi in a "belt and suspenders" approach to improve chances to call out for help during an emergency. You shared reports about home invasions by organized crime using cell jammers to keep intended victims from calling for help. That's alarming. Long ago, I adopted John Farnam's axiom that we're on our own when fending off a lethal-force attack. Still, we're responsible to alert the authorities before self defense is necessary or afterwards once we and our families are safe. That means calling 9-1-1.

Your approach wasn't just cell service plus Wi-Fi – it's a little more complex. Knowing that you've set up robust telecommunications for clients from all walks of life, I wonder what residential solutions would be suitable for middle class clients. Digging deeper into the problem, why would having two phone systems matter? How complex is installing and maintaining that kind of redundancy? Can you get us started thinking about solutions?

King: You'd be absolutely shocked at how accessible and easy to do some of these things are. Most of the time, things that are

[Continued next page]

in the consumer residential market are really not in your best interests, so please don't limit yourself to the residential market. Don't assume that just because something was engineered for the business world, that it's outside of your financial reach.

Let's consider communication depth. I've been reading about cell phone jammers used by criminals. Claude Werner did a report recently where he said from his observations and the news that he's reading, the criminals are coming in packs of three. Is holding your assailant at gunpoint while calling the police for help going to work? I think we have to be very serious in asking, how do we create depth of bench in terms of communications for us and our family?

Let's walk through it. Use your cell phone by all means. Let's say they come with a cell phone jammer that doesn't jam your wireless. Use your wireless. Now, through that wireless connectivity, can you communicate with an intercom or PA system within your facility? What if you have an outbuilding? How are you communicating with the rest of your family? Do you have a speaker in your house to which you can send those communications? How could you do that?

You can't interface a cell phone to an IP speaker to warn the rest of your family. You need your own phone system to do that. People may think, "My own phone system? That's too complicated. I can't do that." I would say, it's not as complicated as you think.

There is a company called 3CX. You can get a hosted small phone system for free. I think it's a 4SC. SC means simultaneous call. There's also technology called Free PBX (Private branch exchange, PBX, an internal phone network that serves multiple extensions in one facility. *–Editor*) There's a free PBX and it is exactly what it says it is, it's a free PBX. There's another one called Asterisk. They have different levels of technical sophistication and technical requirements.

You can do a hosted 3CX phone system for free. I mean, they'll host it for you. You have to plug in a VoIP service (voice calls on broadband internet) to do that, but cost is around 30 bucks a month – very, very cost effective. The cool part is you can use that for a lot of things. If you had 10 family members, all 10 family members could have an extension for which you pay the approximately $30 a month. That seems like some really good economies of scale. There are advantages.

eJournal: Does that replace our landline, Felicia?

King: You bet it does. In fact, I've done exactly that for a large number of customers. Really, though, I prefer having a phone system that I don't need an Internet connection to run, so, if the Internet connection is actually working, great – we have even more functionality. If there's some bad dude with a blocker, I want more communications depth. Wireless and cellular are two different things, and Bluetooth is also different, and RF, CB radio, UHF, VHF, they're all different animals, too. You can't necessarily know what the attack will be, so you can't come up with a bulletproof approach using only one type of communication. There's no depth of bench in that approach. In a bit, I'll get into CB radios and how to incorporate them.

Another advantage of having your own phone system on site comes up if you have a house and an outbuilding or a detached garage. At a minimum, you want to communicate with the rest of your family without them having to pick up a phone, so you want intercom. I want to be able to hit a button or dial a code and literally broadcast a communication across multiple buildings, to the entire facility.

Formulate a Good Plan

King: Define your problem first and then ask, "How do I make sure that my plan allows me to scale it to solve the problem?" When you start, you have to ask, what are the risks you're trying to mitigate? I want to be able to communicate with my family no matter what. I want to communicate to everybody wherever they are inside of the homestead.

A lot of times people get stuck on the technical complexities, and they try to "boil the ocean." Please don't. Define your problem, get some good advice, formulate a good plan, then start by doing just the first piece. That might mean getting a phone system with one speaker. Get that worked out. Once you understand how to do that, you can add as many speakers as you want. Get one intercom. Once you get that figured out, then add as many as you want, where you want.

A lot of times you can do these projects 100% empowered. Here's what I mean by empowered. You have the plan and somebody that you can exchange ideas with and call for advice and say, "I'm stuck. Can you get me past this point?" or say, "I've put together this plan. Look at my plan and tell me where my plan has deficiencies, so it's corrected before it gets executed." If a plan is wrong and gets executed – that's where it gets expensive.

After that, a person can generally do the rest of it themselves. You can run your own wiring, mount your own equipment and fiddle with the programming. There're a lot of things you can do on your own. Like I said, a lot of this is extremely accessible from a financial and a technical perspective.

I want to be able to use a cell phone, but if I don't have cell phone coverage, I need an alternative. Let's try wireless, but I don't mean your ISP's wireless. If you've got a situation with bad guys, you've stopped the threat and are holding one of the criminals at gunpoint, you can't walk away or maybe you don't have the ability to retreat safely. You don't know who is outside. What if your cell phone isn't working and your wireless isn't working because bad guys are blocking the signal? What's your plan at that point?

[Continued next page]

I would plan to use a BaoFeng CB radio. BaoFeng makes these very super, super duper flexible handheld CB radios. You can get a really long 24- or 30-inch whip on it. I've tested the signal distance coverage with the extended antennas, and I've gotten up to three miles depending on terrain and the various frequencies used.

I would argue that CB radio is something that we all should investigate. You can get two or three BaoFeng handheld radios for $60 each. Maybe you put them in your garage, and several other places in your house. It's the same thought process as if you put a landline phone in the garage, back when we had landlines. Think about your CB radios the same way.

Adding CB radio really gives depth of bench to communications. I haven't yet read of a scenario where the bad guys have technology that's so sophisticated that they're preventing your CB radio from functioning, especially if you're using something like a BaoFeng that you can use on VHF and UHF and other frequencies. There's a website about radio communications and related classes at https://brushbeater.org/ . Anybody that's interested in learning about CB could take classes there or just do self-study books. I also recommend the books for getting ARRL's technician class license (https://www.arrl.org/getting-your-technician-license/). There's a ton of information freely available on the internet that's extremely accessible, as well.

eJournal: Another idea for CB radio – maybe we should be teaming up with neighbors for greater broadcast reach. If my home terrain was hilly, maybe I have great neighbors' who live up the hill to which my radio has line of sight, but no farther. I should go say, "Neighbors, things are getting rougher. I hear the gangs are targeting rural homes. We should both have CBs and help each other in emergencies. Would you be part of this neighbor-help net with me?" Now, not only have I reconnected or made friends who might help if our water or electricity goes out, but we've also got someone who could make that 9-1-1 call because the radio up to their house is not being blocked.

King: That's exactly the kind of strategic, proactive thinking I want everybody to do. It is about scenarios, asking what are my problems? How do I mitigate risks? What happens if plan A doesn't work? Can I go to plan C? All of this is completely within the realm of everybody who's a Network member, because of course, what is this adventure of learning the legalities of using lethal force to defend one's life? It's a lot of technically complicated, nuanced things!

Technology is no different. I think if somebody goes to the level where they expend a certain amount of energy and they gain adeptness in their skill set around the legalities of lethal force, they can do so on the technology side, as well.

Part 2. Surveillance for the Home

eJournal: Can we apply the same "start small strategy" to home video monitoring? Not only do we wish, perhaps, to record who came and went, but let's say I see an unexpected truck coming up the driveway. Maybe I want dependents hunkered down in the safe room until I figure out what it is, so we use your intercom suggestion from the first part. If I have video and possibly audio, then I should store what's recorded in case this turns into a home invasion. Now we're getting into a whole other realm. Lucky for us, this is an area in which you've really got some chops. Talk to us a little bit about how we might get video, where we might want to record, and the equipment, the storage, all the things that attach to home video monitoring. I'm going to turn the floor over to you because this is your world, not mine.

King: In my earlier introduction, I didn't mention that I have been a surveillance expert for over 25 years, and I invented a school lock-down solution that is a hundred percent on premise, no cloud dependence so it works just fine when the internet is down. That is how you need to think, too. We've also invented security safety solutions for the manufacturing industry that are surveillance centric, so I have a lot of experience in this area.

Surveillance has a deterrent effect. Just the fact that you have cameras, along with inexpensive signs, is a deterrent. Strategically, it would be great to have cameras that are obvious and cameras that are not obvious, right? If you can include the ability to do IP audio, that's even more fun. Still, we want to make this possible, so we're talking about incremental improvements here.

Let's tie that into a story. Let's say you've got a trespasser on the south side of your property, and they are traversing northward. In an ideal world, an alarm notification indicates the cameras picked up a trespasser on the south side. You need to be able to tell, in near real time, who's outside, where are they, and what are they doing. What is their intent? Where are they going? You need to not only tell that story in real time, preferably, but you also need to tell it "post time."

Think about the Venezuelan gangs that have been in the news in Colorado. The thing that broke that story wide open was a

[Continued next page]

lady's camera footage of them. The video was something she could share. She showed the world this video and it was believable. It was not up for debate. The video can be authenticated. It's not a deep fake.

Video surveillance speaks for itself. When your cameras are strategically placed to tell a story, they can tell law enforcement and the district attorney that the guy started over here, he meandered this way, he was over here this long, he went over this way, he futzed with that, he walked around here, he did that. It's telling a story, and that story is not up for debate.

Your video surveillance system needs to not only have the right placement, the right camera selection and preferably audio, it needs to have the right date stamps. This is really important. Please, for the love of everything, do not manually define the date and time on your devices. Have a system that does that for you.

When you're doing your configurations, you do want to ensure that your video feed has location identifiers – I just use camera names – and a date. It has 2024 dash and then the rest of the date and time, and I mean time down to the second. That's typically called an overlay. It is important. Scenes that generally have a darker or a lighter background need white or black text or maybe you'd use white text on a black box. Make sure that your date and time is readable.

Almost every system has Network Time Protocol built in, so you just need to make sure that you have that configured correctly so the system can reach out to National Institute of Standards and Technology (NIST) and ask, "What's the current time?" Maybe it does that once a day, so you're assured that the correct date timestamp is on all your digital video. That date timestamp has good veracity and would be irrefutable evidence in your favor, reinforcing the story that you're telling about what happened.

We all know from Massad's teachings that human witnesses are highly variable, so the video surveillance becomes that thing that speaks on your behalf. As long as the video surveillance has integrity, it's highly believable. You won't deal with specious allegations from a DA, claiming that something was manufactured.

eJournal: Can we discuss budget decisions like whether to pay for IR cameras to "see" at night? I figure bad things happen at night. I can't see doing video without nighttime capability, but what about a soundtrack? When would we want audio, and where is it unnecessary? Why wouldn't I just source everything with audio?

King: Do I want to have audio embedded in the video that may record an altercation? Yes, I do. A full audio video recording can give me evidence and a whole lot of proof. It's no longer only what I said, now I have this proof that could quickly resolve whether I am going to be prosecuted or not.

eJournal: Just to be contrary, I don't want some of the common devices that process audio in my home because I'm not sure I want Alexa listening to the dinner conversation. I'm sorry, that's just creepy!

King: I only use Axis Communications. Axis is the largest and best manufacturer of surveillance equipment in the entire world that's actually capable of being secured. I've done packet inspections on the behavior of Axis cameras. When I tell an Axis camera to not phone home to the mothership, it does not. When I tell it to only talk to my video surveillance system, it does, that's it. It behaves like I want it to behave. It functions in accordance with real security configurations at the network layer, which, suffice to say, is a technology that has integrity, and it functions in the way that it should. It doesn't do sneaky things behind your back like an Amazon Ring camera or some Google Nest appliance or some other consumer grade baloney would do.

Frankly, almost all the consumer grade baloney is designed to run off a cloud controller and it phones home to the mothership and leaks data, so you have no ability to control or to know what it's doing. I only want to use technology on which I can do a real counterparty risk assessment. It must not talk to anything other than what I tell it to.

eJournal: We sometimes end up with low-end consumer-grade tech from a big-box store because we found an unbeatable bargain we couldn't pass up. I'm sorry, but that is how we stumble into problems like this.

King: I should talk about duration and sustainability of security equipment. I have had cameras that have lasted for 14 years, so please do not tell me, "My gosh, the camera's too expensive!" What's expensive is garbage technology. Good technology lasts a very long time and it's secure-able and it's actually going to be reliable and function. The last thing I want is a scenario where I've purchased an Hikvision camera and just when I needed that camera to work, it malfunctioned, or it was compromised or in some way didn't fulfill its mission. If that happens, I might as well burn the money I spent on it, plus my labor and supplies and everything else because the component failed.

[Continued next page]

I'm not saying ride the equipment until it dies, but don't assume that equipment with a five-year warranty is going to die in five years. It's OK to use it until it dies but have a capital reserve account for lifecycle asset management, because this is now a key component of your infrastructure. You do want a life cycle asset management process, but good cameras like those from Axis are not throw-away devices.

When you choose good technology, it is not proprietary. This is important, so think about it. Somebody says, "Well, I'll go to Walmart and buy this system. It looks inexpensive." First, it's going to be impossible to secure it because it was not designed to be secured. The other problems? You're probably not going to be able to read the user manual for it, and the life cycle asset management on this stuff is going to be atrocious.

Here's the worst part: it won't work with anything else. Remember, you want a design that you can start with one asset, maybe a camera. You want that to interface with a speaker you get later. Later, you may want it to work with a pin pad, and a gate controller and with your video management system, which is just some software on your PC. You want it to work with your phone system. You want all this interoperability. You get all this functionality by using technology that adheres to standards. It functions the way that a network security architect like me would look at and say, "Yep, that's the way it's supposed to work." You want to buy equipment that adheres to international standards, not something from some manufacturer in China.

Here's another thing that's awesome about Axis Communications: let's say you buy a camera, and get a video management system (VMS), they give you a free Axis camera station for one camera. Your Axis camera station license is perpetual, you're not renting the license. I still have the ACS licensing that I had from 24 years ago, although I obviously have more licenses now. This is part of the economic viability. You're paying for perpetual licenses, not subscription fees. It's very, very economical. For the video management system, go buy a PC with a two-terabyte hard drive and install the software. You don't have to have a special appliance for it.

Is it a little bit more complicated than that? It can be. When we do implementations, a lot goes into the engineering and specs. We can do full management of systems to secure them and maintain them, or we can have a collaborative relationship and say, "Okay, you drive, but we'll advise you remotely." We're pretty flexible.

If somebody wanted to do it on their own, they could just get the video management system software, buy the perpetual licenses, install it on a PC and wing it, right? You can totally wing it. One key piece is to make sure that it's not phoning home to some mothership on the internet someplace.

Camera placement is another key piece. You have to be cognizant of the scene. For example, what if a camera is directly facing eastward? It is going to take the sun right in its face and be blinded. Maybe you need a little sunshade for it, so as you're picking out your cameras, you'd look for a camera that has a sunshade.

If you're going to put a camera on the outside of a building, make sure it's outdoor rated. I also want an integrated IR illuminator, which is infrared, to do video at night. There's usually only about a $100 price difference so my general rule is to always get a camera that has a built-in IR illuminator unless, for that particular location, a built-in microphone had higher priority and my budget couldn't support both. There are cameras that have both, but sometimes you have to make a choice because of economic factors, right? On Axis's website, they have a camera selector and if you spend enough time with it, you'll probably do okay.

It's like picking out any other technology. There is a tad of experimentation to it, and you just have to be okay with that. However, if you're just starting, don't buy 12 cameras at once. Please don't try to "boil the ocean." Get one camera and then hook it up and learn how height and other things affect scene composition. There's no substitute for your own experiential engagement! With the systems that I advocate, you can just get one camera and you can start puny small and not lose anything going forward.

In time, if you want to go gangbusters and get 26 cameras, call me because I'll get you discounts. Don't go out and buy 26 cameras piecemeal because you're not getting good discounts that way. By the time you get past four cameras, I'd imagine you understand a lot more from your own experience. You'll have learned about things like "panoramic" or "360" cameras you mount on one side of a peak of a building. It obviously doesn't see

[Continued next page]

behind it, but it sees 100% of everything in front of it: the walls of the building that it's mounted on, all the way around. Those cameras can have their positives and they have their negatives, so oftentimes we'll team them with different cameras for different purposes.

There are cameras that have something called object tracking that are super-duper cool to put on like a peak of an exterior building facing a driveway perhaps. They're much more sophisticated, costing about $1,000 dollars, but still not horrendously expensive, not like a $5,000 camera, right? If you're interested, the phrase that you want to look for is "digital object tracking."

You have to program digital object tracking. As an example, here comes a car. Now, when I see a car on my facility, I want to zoom in and get the license plate. I would also like to get a face shot of who is in that car. You could do that with a two-camera combination, or a more advanced camera. There are dedicated license plate reader cameras, but I would only put that in a business. License plate recognition is a whole separate security topic.

eJournal: It's beyond what many of us in the "getting started" phase should get tangled up in.

King: What you don't want to do is rely upon just one completely visible camera that makes it completely obvious to the bad guys that if they take a can of spray paint to it or kill it, then your game is over. So have some depth.

eJournal: Whether it is one camera or a dozen, if you recorded and stored images of the people who destroyed it, you might have something useful.

King: You mentioned storage earlier. Alright, then, let's talk about storage in depth. It is important because I can't necessarily count on how an investigative team is going to respond to a situation, so I want to make sure that I am not left without evidence. I'm not going to get into politics, but people may recall what happened to Roger Stone. The FBI came in and they took his digital video recorder. That left him without his video.

In a home defense scenario, might an investigative team seize the video equipment if they think it is pertinent evidence to the investigation? Do you want to be in a situation where your defense team doesn't have the video evidence? Well, personally, I don't, so I put SD cards or micro-SD cards in each individual camera, and that's an on-camera recording you can also send to your own video management server. Let's say the VMS is in your building. You can also have that data replicate offsite. There are a variety of ways to do offsite replication, but I won't bore you with the details. If I have the option to store that video on the device itself, but also in a video management system, also stored offsite, have I increased my probability of having access to that video or that event data? Yes, I have.

Now, let's take it one step further. What if you had email notifications configured with snapshots? This is super cool. Let's say you went to the doctor's office, and you just want to find out what's going on at home. If you try to pull up the video feeds from your house, you've got some technical challenges. Number one, if you're going to allow access from the internet to your video management system, you've got some security concerns that are frankly above your pay grade.

eJournal: I defer to you! If I want remote viewing, you are hired to oversee installation.

King: That is my realm. Please for the love of everything do not make your video management server accessible to any externals. Don't do that. Please do not do that because then the stalkers can get into it; the Chinese can get into it. Okay, let's just take that off the table! You could inexpensively configure email notifications that don't open that vulnerability.

For example, a bad guy trespasses on the south side and triggers an alarm. That alarm makes your VMS grab a snapshot and send it to you in an email. You could perhaps have a shared mailbox with your family or spouse, so the notifications are sent to a shared mailbox that can effectively be an archive, too, with a retention policy that automatically keeps only the last four months of snapshots and email notifications. That's another very, very inexpensive way to create a trail of evidence that shows, for example, the bad guy going to the east side, then a snapshot if that bad guy goes to the north side or he goes to the west side. You've got snapshots of where he went. It is all about how you configure the triggering.

Pretty much every camera has motion sensors, but not in the way that you might think of a standard motion sensor. The camera senses pixel changes. This is really important: motion in video surveillance is almost exclusively triggered based upon pixel changes.

If you had a trigger based upon a car driving by, realize that a car is a fairly sizable object. A car is going to change a lot of pixels at a time, but if we've got a guy off in the distance, he's only two millimeters tall on the video, right? That's not many pixels. As he gets closer to your house, he's now four inches tall on the video. That's more pixels. The larger the object, the longer the duration that it has changed – that is what triggers

[Continued next page]

motion. You will have to tune this for each camera because each scene is different. If you've pointed a camera at your garage entrance, that's a very different scene than a camera pointed at the sidewalk in front of your home.

Speaking of sidewalks – and really a lot of other scenes that you might think of – you can create areas of focus if you want. I had a client who was very concerned about potential tampering at his well but didn't want an alarm going off whenever anybody used the driveway. He just wanted activity around the well head to generate an alarm. He can set that trigger zone at the wellhead as simple as opening up the VMS, drawing a little box around the object that he wants to monitor and creating a motion alarm for that. Not hard at all.

eJournal: A common complaint about simple motion alarms is deer, birds and even spiders setting off the alarm. You've just shown us how to monitor only the area we're worried about – a gateway, short length of driveway – without getting alarms from other, benign activity nearby. If we can decrease false alarms, more people will use motion detectors.

Suppose it is a trespasser? How are we moving the video from the camera to trigger the notification, and transfer it to the storage, too? Can we also store audio? If it is a fake delivery person, it might be useful if we record him or her saying, "Let me in so you can sign for this package."

King: Okay, so we'll get a little technical here. When you're programming a camera that has audio capabilities, you tell it to record the audio with the video. The audio is just another channel on the same video feed, they're matched up and either you have audio, or you don't. Video and audio are live streamed from the camera to the VMS. The camera doesn't record it then do a handoff, it's live streamed to your VMS nearly in real time, with only a few milliseconds of delay.

Get familiar with any sort of delays in your system because you need to know how long the delay is between beep and when the person is at your door. I use a bit of a depth in my approach. I have driveway alarms. I think when people have gotten motion sensor driveway alarms and have a lot of false positives, maybe they didn't do the right device selection. There's a magnetic underground alarm you bury that's near 100 percent reliable. It's a giant magnetic sensor that goes off when a vehicle drives over it, but you have to dig up your driveway and put it underneath it. Because it transects your driveway, you also have to get a wire out to it. There are a variety of approaches, including underground pipes, which we can talk about later. That's super reliable, but costs more.

For less, there is a radio frequency alarm from Chamberlain, the company that makes the garage door openers. It's consumer grade tech but doesn't use wireless internet. The little Chamberlain units are just battery operated and have a hood that keeps out a lot of the false positives. The other thing I like is its little rectangular sensing area, like a viewing box. It's like looking through binoculars.

When you set this thing up, you have to put it at the right height. You have to point it directly where you want motion to set it off. You're basically telling it, "I want you to only look at what's in this little viewing box." You can tune that really well. That little Chamberlain unit is $60 or $80. We're talking about pretty inexpensive stuff.

Now, the thing I really like. Is it fast? Yes, I mean, it is real-time beepification! That can be super-duper handy, right? This is depth of bench we're talking about here. Something comes down my driveway, I would like to have a real time beep to get my attention so that I know something is there. Then I can maybe pull up my video surveillance and take a look. I would have had more delays if I used something without instantaneous beeping. I really want that notification in real time.

Think about "swatting." Someone makes a false allegation – a caller says that there's a kidnapping inside of a building or something – because they're trying to get you whacked. If the SWAT team rolls up at 2 a.m., I want the beeping to let me know. I can pull up my video feed and recognize what's going on outside so I can respond to it appropriately. Otherwise, I might be dead. If that thing goes off at 2 a.m., I'm waking up and I'm paying attention to what's going on.

If you're thinking of turning off the motion detector because of too many false alarms, consider the risks. You're trying to mitigate the risk of not having enough advance notice to deal with something where life or death is at stake.

If your detection system has a lot of false positives, you need to spend some time tuning, rather than just get rid of it. Play with it, mess with it, find out how it works. Personal security always requires tuning, that is why I think it's so important that people try to not outsource all of this. It really is no different than learning how to defend yourself. You're not outsourcing that, are you? This is the same thing, because only you are able to make an assessment about your risk tolerances.

eJournal: Returning to the video storage issue, what options should we think about?

King: The technical piece of it is basically this: the camera writes to the micro-SD card and the VMS is pulling that video in real time. Offsite, like I said, can happen a variety of different ways with different technical prerequisites. Depth of resiliency is a bit of an art form.

If you came to me and said, "You know, Felicia, our internet connection is not so good, but I would like to make sure I don't lose security video if somebody came into the facility and either destroyed or took my VMS. Can we mitigate that risk?" I would say, yes, and we would probably get you a small, affordable

[Continued next page]

NAS (network attached storage) and do file writing to an SMB (server message block) share on that NAS. We would put that thing in what I'm going to call a non-obvious location.

This goes back to the old axiom, don't have your server with the backups right next to it. If your video management server is in one place, let's have your resiliency video storage location elsewhere in your building, or maybe in your outbuilding or garage. Setting up the stuff there is just a one-time expense to run a cable, so don't be afraid about that either.

eJournal: Many have locking cabinets or closets where it would be sensible to secure the backups, as a failsafe, just to make sure.

King: The risk management piece is you don't want to lose your data. You don't want someone else to be able to alter your data. You absolutely must deeply safeguard against inappropriate access to your video.

eJournal: That's one fear that turns away highly private people. They simply won't put up any surveillance devices for fear of unauthorized access. That's my biggest argument for having someone like you spec out the initial design. Another issue arises for renters when we talk about pulling wire or trenching under the drive. How much of this scales for people who are renters?

King: Actually, quite a lot of it. I do property management for commercial property management organizations, like large apartment complex owners. If I was a renter, I might go to my landlord and say, "Let me propose something. I want to draw up my own plan and fund the professional installation of home surveillance. Okay?"

If I'm the landlord, I don't want something that is tacky, and I don't want to see rogue stuff or surface-mounted garbage. I would much prefer the tenant come to me and say, "Hey, let's do some cost sharing here." Ask the landlord, "Can your contractor professionally run wires in accordance with your standards through your walls? I'd specify where I would like them, and I will agree on what I would leave in this unit if I departed." Amicably come up with a plan that addresses the landlord's concerns. Have a respectful conversation, so you can have what you want and respect their property. Don't go in and say, "I want you to fund the surveillance inside of my apartment." That's not an equitable plan.

eJournal: Imagine being the next tenant to move in and wonder, "Gee, I wonder what the person before me was doing?" Hopefully, the next tenant would know how to use it, so it wouldn't be wasted. How universal or how rare is installing surveillance becoming, Felicia?

King: I would say it is standard operating procedure now in any large apartment complex, especially for middle income or upper middle income. Video surveillance is something a lot of tenants request or demand. They are exceedingly sensitive to the assurances that the system operates completely independently with no phone home to the mothership and no mechanism for the landlord to spy on them.

Management of your own system in your own home is different than what we have to do for a tenant in an apartment building. We can give the tenant the system, but we can't as easily support them, nor can we as easily enable them to have secured remote access.

We also don't want anybody on the internet to be able to get at your video surveillance system. I about lost it one day when a guy had told me that he had put Google Nest or Amazon Ring cameras in his daughter's bedroom. I think she was rather young, and he was not a perv or anything like that, but it's just not good risk management. It is just going to be exploited by the hackers.

eJournal: How can we get remote monitoring without creating the dangers that poor dad did?

King: Don't enable remote access to your video surveillance system unless you can restrict that exclusively to your designated, authorized access. That's truly imperative and can be done with something as simple as an appliance at your house that you own or that's managed for you.

For example, I can push a button on my smartphone phone, and my phone will initiate a secure tunnel to my network. This secure tunnel is almost like you and me picking up cans with a string between them and playing the game of telephone. The tunnel makes those communications privy only to the parties of that communication. That enables you to be at the dentist or the ballpark and be able to investigate what has transpired at home through video recordings. You get an email notification and a snapshot that's interesting, you can drill into it without driving home.

eJournal: Your advice about protecting surveillance from prying eyes reminds me of your ideas about practical ways to hard wire connections to remote access gates and intercoms to detect threats before they ever get close to our homes. We need to talk about that, too. Let's do that next month.

Thank you for taking us this far! There's a lot more we can do to keep an eye on what's coming up to the house. Let's return to this and related subjects next month and ask you more questions about these and other personal security issues. I know also that you have a great philosophy about tackling large, intimidating projects for those of us who feel incompetent in the tech space. I look forward to sharing all of that and more with members in our December online journal.

President's Message

by Marty Hayes, J.D.

I was having breakfast this morning with Belle McCormack, the owner and director of The Firearms Academy of Seattle which is the training company I used to own, before the Network took over my life. I hired her to run the academy about five years ago, when I could not do justice to both the academy and the Network at the same time, and then sold it to her about three years ago.

Belle had just completed an Advanced Tactical Handgun course, a course of instruction I designed over two decades ago to allow students the opportunity to experience the type of training that police officers receive in the standard state-run police academy, which consists of not only handgun skills range training, but also training in decision making, hostile threat mitigation, weak-handed training, low light training and a number of other experiential training exercises. You see, it was and still is my belief, the armed citizen should have the opportunity to seek out the very same type of training that law enforcement officers receive before going out into society and facing the criminal element.

The reason for this belief is that the armed citizen faces the very same criminal element that law enforcement faces, except the armed citizen typically has no body armor and no back-up officers either on-scene or on their way. The only real difference is the police are called to interact with the criminal element or paid to go out hunting for them, and hence police are more likely to have to use deadly force than the typical armed citizen. Still, make no mistake, the type of criminals and the threat is the same.

Anyway, back to my breakfast conversation with Belle – she was relating the different things that happened over the weekend, and it reminded me that I really should write about the topic in our members' journal. It is my intention that our members should take a solid assessment of their training experiences and the skill level they possess. Have you been trained to shoot at moving targets or in the dark? Can you operate your carry gun weak-handed, including reloading it and clearing malfunctions with only your weak hand? Do you train to face multiple threats, and do you practice long distance shooting?

In addition to the above, the other type of training I am convinced that the armed citizen should experience is a good dose of "force-on-force" training, what we called back in the day "mock scenes." In police training, mock scenes typically involved traffic stops (including felony stops), building searches, and handling domestic violence situations – all part of a police officer's normal work. A good full day of training in the FAS Advanced Tactical Handgun course includes these types of scenarios, including bank robbery scenarios, convenience store scenarios, home defense scenarios and more.

You see, the philosophy behind putting the student in these simulated encounters is that by giving them realistic experiences in training, if they find themselves caught up in a similar situation for real, it will not be the first time they have faced such a problem. I know that if it were not for the training I received in my police training, I would not have been nearly as confident as I was when I had to make my first felony arrest. All I had to do was to do it how I had been trained, and all worked out fine.

To my knowledge the only other training schools that I can recommend to expose you to this type of training is Gunsite Academy in Arizona or KR Training in Texas. I am not as familiar with Network Advisory Board member Karl Rehn's KR Training curriculum as I would like to be, but I have been a student in at least one Gunsite class yearly for the past decade.

As of this writing, we have about 22,000 members of the Network, and while we do what I think is a very good job teaching and educating members about the legal aspects of use of force in self defense, what we cannot do in our current structure is teach the hands-on aspects of deadly force training. I am open to suggestions on how to expand our training and education into these areas. Just to clarify, I am not talking about starting a shooting school or certifying instructors. To do so would take our attention away from the work the Network currently does. Is there, instead, some way to replicate the hands-on force on force training by using current, modern technology on a wide scale basis? If anyone has any ideas, please reach out to me.

Attorney Question of the Month

This column focuses on demystifying legal defense issues so members better understand what they may face if they use force to defend themselves or their families. Defense against road rage is the subject of this month's Attorney Question of the Month in which we asked our Affiliated attorneys the following:

Here's the scenario:

A man, let's call him Steve, driving on a freeway is aggressively tailgated, then almost forced off the road by a driver who pulls his pickup and trailer up even with Steve and into his lane. In this road rage incident, Steve's front facing dashboard camera records Steve steering onto the paved shoulder, but then steering into and intentionally striking the other vehicle out of fear he is being forced into the ditch and where he may be killed. This raises the question below--

In your state, would the courts consider an argument of self defense if, in response to a road rage attempt to force you off the road, you steered your vehicle into the initial aggressor's?

Timothy A. Forshey
Timothy A. Forshey, P.C.
1650 North First Ave., Phoenix, AZ 85003
602-495-6511
http://tforsheylaw.com/

As with most everything in the law, the answer here is "it depends." In short, in my home state of Arizona (and, for that matter, in every other state and in most nations) one can legally use lethal force "when one reasonably believes one is in imminent fear for one's life." Here, if the success of the attempt to force you off the road would likely be fatal, then resisting that attempt should be legal. I know at least one jury agreed with me.

Several years ago I had a client who was driving his vehicle with his infant daughter in a car seat in the back of his vehicle. As he lawfully exited the freeway via a 40 feet tall elevated offramp, a bus driver (operating an otherwise empty bus, thankfully) realized he was in the wrong lane and that he needed to be in the lane occupied by my client's small car. As we have all experienced with large trucks/buses, he simply started into my client's lane, assuming that the smaller vehicle would give ground out of fear of being (forgive the use of Latin here) smushed. When my client unexpectedly failed to yield, the bus actually started smashing into my client's vehicle. Rather than simply "steering into the aggressor" as in our hypothetical here, my client fired three 10mm rounds from his Glock 20 through the bus's windshield, two of which hit the bus driver in the face. Thankfully, the bus driver survived, albeit with a severely altered profile. The evidence clearly showed that the bus driver was the "aggressor." The first trial was declared a mistrial due to a hung jury, but the second jury acquitted my client.

Lest anyone think this was a "victory," let me point out that my client (who spent four months in jail pending my efforts to get his bond reduced), as well as his parents, lost essentially everything they owned before the dust finally settled two years later. My client's girlfriend also left him with the infant daughter in question. My client (who calls me every year on the anniversary of the shooting) has gained 100 pounds and been unemployed ever since. The "victory" was devastating. Maybe simply allowing the bus driver to take the lane in the first place would have been a better idea. My client could have made that choice. The law did not require him to ("stand your ground"), but he could have yielded had he been willing to swallow his angst. I always suggest in such cases of appropriate restraint that you immediately thereafter offer up a quick prayer that the other person awakens tomorrow with a hemorrhoid the size of a volleyball – and let it go.

The moral of the story is that responding with lethal force should never JUST be "justifiable." It should be justifiable AND UNAVOIDABLE. When you ask "can I legally shoot this person (or attempt to run THEM off the road instead) if they are doing X to me," you are missing the point. You must believe, nay, you must KNOW, that your failure to do so will result in your death. Then, it becomes your lawyer's job to get the jury to agree that they would have reached the same conclusion.

Craig R. Johnson
Craig Johnson Law, PLLC
2500 N. University Ave., Provo, UT 84604
801-458-2285
https://craigjohnsonlaw.com/

Absolutely! In Utah, it specifically excepts those that:

"...initially provokes the use of force against another individual with the intent to use force as an excuse to inflict bodily harm upon the other individual..."

Other than that scenario, Steve is justified in taking these drastic measures to avoid his own serious bodily injury or death.

See: https://le.utah.gov/xcode/title76/chapter2/76-2-s402.html

[Continued next page]

Don Hammond
Criminal Defense Heroes, P.C.
1327 Post Ave, Suite K
Torrance, CA 90501
323-529-3660
https://www.donhammondlaw.com/

I would not expect that to be a good defense. I think the obvious answer is that the "victim" should stop his vehicle, creating distance from the aggressor vehicle and thereby defusing the situation. Any aggressive reaction such as steering into the other vehicle will escalate the situation and lead to a "he said/he said" situation regarding who was the initial aggressor. Proving who initiated the aggression will be very difficult, time consuming, and expensive.

This can all be avoided by stopping the chain of aggression. Once Steve is on the shoulder and the other driver is continuing down the road, there is no continuing threat to human life to justify using force in self defense.

Robert E Calesaric
Calesaric Law
35 S Park Place, Ste. 150, Newark, OH 43055
740-973-6800
https://www.calesariclaw.com

You definitely have a self defense claim. In fact, in Ohio we now have a form of a stand your ground law.

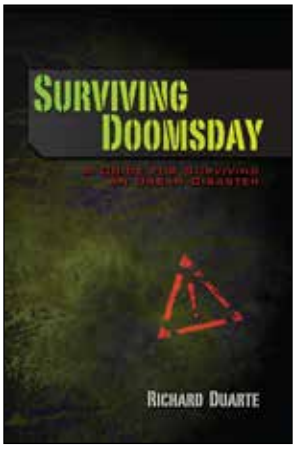
_____

Thank you, affiliated attorneys, for sharing your experience and knowledge. Members, please return next month when we will explore a new question.

Book Review

Surviving Doomsday:

A Guide for Surviving an Urban Disaster



By Richard Duarte
CreateSpace, Dec. 2012
Paperback, 181 pages, $18.95, Kindle, $5.99
ISBN 978-1480270664

Reviewed by Gila Hayes

As a follow up to August's book review, this month I studied another author's work about preparing to survive natural disasters, grid down and civil disruptions all falling under author Richard Duarte's categorization of "WCS – worst case scenarios." Realistically focused on what city-dwellers can do, *Surviving Doomsday* is an older book, but is packed with solid, workable solutions for water, food, first aid, self defense, deciding to flee or stay put, getting home in a crisis and more.

Duarte theorizes that people are shocked when an emergency strips away food, water and shelter because "most of us have never really been without the basics, and our attitude reflects it." By contrast, early homesteaders dug wells, gardened, farmed, raised livestock and if a disaster wiped out their homestead, they got to work recovering and didn't wait for help.

In urban and suburban survival scenarios, you, too, are likely on your own. "During the initial period after a WCS, you will most probably only be able to count on yourself and the preparations you have made," Duarte urges. For example, consider our reliance on petroleum, he writes. If war or natural disaster disrupts oil production, freight stops moving and merchandise will disappear from local store shelves. What happens then?

Stockpile water and food before others panic, Duarte suggests. Grocery stores usually need to restock at least every 72 hours, but shelves empty more quickly when fears arise. If freight trucks stop rolling, not only will physical hunger foment trouble, the psychological and emotional backlash amongst a self-indulgent population obsessed with eating when and what it wants will be substantial, he warns. "During a WCS you'll need a mix of carbohydrates, protein, fats, vitamins, minerals and electrolytes to stay on your game. The moment you start to reduce your caloric intake, you will also begin to see a marked decline in your physical and mental performance. It's your job to make sure you plan ahead so that this doesn't happen to you."

Duarte acknowledges that "very few people have the time, money, space or even the desire to purchase, store and manage many years' worth of food." Urban apartments, he notes, have no available space for the bulky long-term stored foodstuffs. "The idea is to have enough food to allow you and your family to survive a short-term crisis within the relative safety of your own home or some other secure location," he explains, recommending that food set aside for emergencies "should always be 1) shelf-stable, and store well ... 2) easy to prepare and consume ... 3) generally require no cooking, can be eaten cold, or warmed up slightly 4) fit nicely within your budget and 5) easy to rotate and use on a regular basis," and, he adds, don't forget to have two can openers – redundancy is advised.

Don't stockpile food without knowing it is palatable, and packaged in servings that can be used up before it spoils. He suggests calorie-rich foods that store relatively well without refrigeration including peanut or almond butter, canned meats, fish and seafood, pasta sauce, evaporated milk, fruits, and vegetables. Dry goods include rice, beans, oats, powdered milk and protein powder, granola and protein bars, dried fruit and nuts, pancake mix, and pasta. Dark chocolate, instant coffee and honey and sugar round out his suggestions. Storage containers must protect emergency foods from bugs and rodents, moisture and humidity, he warns. Regular food rotation is a must. MREs and camping food pouches work well for bug out bags, he adds.

Water leads Duarte's concerns, and his minimums are higher than most: two gallons per person per day, kept fresh by stock rotation, or purified through a variety of methods. He outlines the symptoms of dehydration and discusses making water safe with bleach, iodine, UV purification or boiling. Increasingly, Americans live in big cities, reliant on municipal water systems, many of which are outdated, overwhelmed, and failing. "In order to survive a WCS in an urban environment, your water plan will require your full attention and some substantial planning, far in advance of any unexpected event," he stresses.

Sanitation and hygiene during a worst-case scenario receive a full chapter in *Surviving Doomsday.* Normal conditions make hand washing, waste disposal and bathing so easy that we forget how dirty hands spread MRSA, E. Coli, Norovirus, salmonella, fecal bacteria, and more. Besides drinking water, you need disinfected water for washing, plus antimicrobial hand sanitizer (to cut down on clean water use), chlorine bleach, disposable plates and utensils to limit dish-washing, and paper towels so cloth towels don't spread germs. Even baking soda and white vinegar aid in cleaning. Wear surgical gloves and masks when helping sick people or cleaning the latrine and have sealed plastic bags in which to dispose of feces or diapers placed in covered containers far away from living areas.

Duarte discusses first aid kits "designed to treat either a non-emergency situation that does not require a doctor or hospital, but may still require care to avoid complications, or to treat an emergency situation that requires instant care until the person can be taken to a doctor or hospital," recommending staging kits in your car, home and workplace Most first aid kits sold "are filled with a lot of fancy packaging and very few truly useful products," he observes. While a commercial kit encourages some to start carrying first aid supplies, it is best to build your own kit so *Surviving Doomsday* sketches out an extensive list ranging from tourniquets to chest seals, bandages to Steri-strips, and much, much more.

[Continued next page]

"Having medical supplies and medications and using those supplies correctly are two entirely different things," advises Duarte, recommending training and having your own doctor's advice about medications you can or cannot use. Stay current on vaccinations before an emergency and maintain dental health, he adds, so you start strong if a crisis arises.

Don't tell others about your preparations. When desperate people forage for food, water and shelter, your stockpiles will attract attention unless you practice strict privacy, Duarte writes, in one of *Surviving Doomsday's* repeating themes. Beyond hunger, "also expect dramatic increases in the activities of criminals, who by their very nature, will be inclined to prey on the weak, much as they do today, but in the absence of law and order, to a much greater and more violent degree," he writes. Stay in your home where you are safe from human predators. "During a WCS, it's not your job to go outside and fix the problem(s). The magnitude of any such problems will be beyond the capacity of any one person. Your job is to deal with and manage the effects of the situation within your own home."

Keep your home locked and don't attract attention. This is a team effort, Duarte writes later, recommending that everyone in the home understand home defense and shoulder elements of it appropriate to their abilities. Stay indoors and only allow immediate family inside the home. Keep your supplies hidden. If compelled to share, draw those goods from a separate cache, not the one on which your family depends. Before an emergency, reinforce doors and windows, hinges and locks, and trim or remove bushes, but add low, thorny ones around the windows as deterrents. Set up and supply a safe room and establish a code word to trigger immediate retreat by all family members.

Duarte highlights the value of good tools, observing that in emergencies stores run out or inflate prices of chain saws and simple construction tools and supplies to repair damage. Tools and know-how to shut off your home's gas lines and water mains are important, he adds. Your emergency tools should never leave your homestead because borrowed tools are often returned broken or not returned at all. Buy the highest quality you can afford, from axes and shovels, to chain saws, power drills, generators and portable heaters or coolers, he urges.

Most of *Surviving Doomsday* is about preparing to shelter at home throughout a crisis. Duarte explains, "Absent extraordinary circumstances, your home will usually be the safest place to be during and after a major crisis. If you have planned well, your home will afford you food, water, relative security and the home court advantage." Preparation for circumstances that contraindicate remaining at home is discussed with lots of caveats.

The common "head for the hills" fantasy is extremely unrealistic, Duarte stresses. "Absent some very hardcore survival training the majority of us average folks will not last more than a few days in the wilderness." Often remote wilderness is too far away, sufficient supplies too heavy to carry (a gallon of water weighs over eight pounds), and automobile travel is often untenable in a crisis. If you must leave, Duarte writes, depart as soon as you learn of the danger before gridlock blocks the highways.

Determining whether to "bug out" pivots on having a place to which you can flee, whether you can walk or bike to it, or, if you need to drive, can your car manage the terrain, and do you have enough fuel to get there? Do you have safe resupply and rest points on the way? Are there several routes to your destination if some are blocked? Know these things in advance and if you must flee, have a packed bag ready and don't delay.

Commercially compiled bug out bags rarely meet individual needs, Duarte continues. Priorities include ease of carry if blocked roads prevent fleeing by car, and a bug out bag's contents should be appropriate to the weather, include a compass and local maps, plus about two dozen other items specified in a list of suggested "carry with you" necessities. Practice is crucial, he writes, so, for example, if you've not used a map and compass, now is the time to learn. Pack items most likely needed on top. Bug out bags should be unpacked, refreshed, and repacked at least once every three months, he urges.

The bug out bag's counterpart is the get-home bag, Duarte continues, discussing supplies to carry all the time. The survivors walking home after the 9-11-2001 attacks on New York illustrate the unpredictable need for serviceable shoes, flashlights, food bars, water, first aid supplies, plus a dozen and a half other items listed in *Surviving Doomsday.* The biggest challenge is consistently taking along a get home bag because, he warns, "the day you need it, you will need it desperately."

Emphasis on equipment, supplies and gear, can eclipse the crucial factors of fitness, health, and mental fortitude, writes Duarte. Emergencies test strength and stamina when survivors may need to carry an injured person or clear fallen trees blocking a door. "Urban survival is as much about preparing physically and mentally, as about security, water, food, and medical supplies," he writes. "All the stockpiling in the world won't help someone who is mentally and physically unprepared."

Test yourself, Duarte suggests. Can you turn off power and water and rough it at home for 24 hours? A week's worth of life's challenges can tested in one day. Turn off power, water and gas, use a sanitary toilet solution and outdoor shower, water purification, do meal prep that wouldn't draw in predators with the scent and doesn't require electricity, and hand-wash your laundry. Simulate an injury requiring first aid, have family members keep security watches 'round the clock, and turn off heating or cooling to experience how local climates affect the family if electricity goes out for a long time.

Duarte synopsizes the supplies he discussed in the previous chapters into comprehensive lists covering water, food, medical, clothing, bedding, tools and equipment, hygiene, and defense. *Surviving Doomsday* closes with these extensive lists, a glossary, and a recommended reading list for further study.

Editor's Notebook

by Gila Hayes

We suffered a big loss in mid-October when Ed Lovette passed away. I was so very fortunate to meet Ed in person at a writers' event at Sig Sauer Academy many years ago. Although a regular reader of his columns in *Combat Handguns,* that was the only time I was in his presence, but Ed stayed in touch and we corresponded occasionally and spoke by phone now and again.

In addition to his thought-provoking columns in *Combat Handguns* magazine (back when glossy magazines were delivered each month in the mail), Ed co-authored an excellent personal safety book, *Defensive Living*, with Dave Spaulding. Ed is best remembered for his book *The Snubby Revolver,* first released in 2002, which he updated significantly in 2007 and again 2021. A retired CIA paramilitary operations officer, Ed understood that his career was a great training grounds for the mission of teaching private citizens how to go armed and be prepared for self defense because of the "invisible," covert nature of the CIA officers' on-duty time. He was particularly focused on extreme close quarters defenses, although, in my opinion, his coaching on threat detection and avoidance, as well as mental preparation, was unparalleled and should have received much more acclaim. I experienced Ed as a quiet, reserved man who would speak out with authority about what he knew but he was never one to seek the spotlight.

Our community is the poorer for his passing. Fortunately, Ed left a great collection of knowledge behind in his books. In the spring of 2019, he generously gave me a long interview we entitled *Beneath the Radar.* I would love it if members honored his memory by reading and putting into practice the key principles he shared about not attracting and how to deflect a predators' interest at https://armedcitizensnetwork.org/beneath-the-radar .

Be A Better Citizen

There are only a few days left before what I have come to believe is the most important presidential election in my 60-something years on the planet.

My home state mainly votes by mail. Suspicious soul that I am, most years I wait until a day before the deadline to fill out my ballot and put it in the drop box or mail it back. I am only half-joking when I quip that I wait until right up to election day before voting in case a horribly disqualifying or disgusting detail emerges about a candidate at the last minute that would make me change my vote.

I'm changing procedures this year and filling in my ballot a little early. I took my ballot to the county auditor's office in person this year, out of concern it might be lost in the mail or maliciously destroyed in a ballot drop box. In our end of the county, the ballot drop box is in a far corner of the elementary school parking lot and frankly, it is extremely vulnerable to damage. Likely I am being silly and nothing malign will happen to ballots left there, but to me, the risk isn't worth the convenience of stopping by the school parking lot after work and sliding my ballot envelope through the slot.

I have strong opinions about candidates in a number of the races in this election; you likely do, too. I'm not going to try to change your mind. One characteristic of my parents' generation that mine has somehow lost is knowing how to respect opposing opinions. I'm trying to do better. What I will ask of you, though, is please, members, do your civic duty and cast your ballot.

Civics!

Could you pass the citizenship test required of new immigrants? There are several sets of 20 practice questions that are fun to go through at https://www.uscis.gov/citizenship/civics-practice-test-2008 .

For several years, the U.S Citizenship and Immigration Services has been promising a selection of updated test questions, but the 2008 version isn't bad, really. I wonder how many high schoolers could pass the test? For that matter, how many of our acquaintances and business associates could? I wondered if I could get 100% on a practice test. I missed perfect scores by one question about half the times when I ran through several iterations of different online quizzes, but then I'm so old that I actually got graded on civics classes when I was in school.

Check out the practice test for yourself. It is kind of fun to see how much you know and equally useful to learn if gaps in your knowledge exist. Some sample questions are pretty easy, and while we might wish we didn't know their names, we generally know who is president, vice president, our state senators or the name of the Chief Justice of the United States. I was less certain when asked to pick the name of the president who served during World War I. Had the test been fill in the blank, I probably would have failed that question. The four choices included three presidents from what was clearly the wrong time period, so "multiple guess" saved me from not knowing my American history as well as I should. I also was a little unsure about the century in which we fought the Mexican-American war, so once again, I'm seeing that I need a good book or two on American history.

Questions are Good

In closing, let me share some words to live by that I recently saw in a member's sig block: "I would rather have questions that can't be answered than answers that can't be questioned." *--Richard Feynman*

About the Network's Online Journal

The ***eJournal*** of the Armed Citizens' Legal Defense Network, Inc. is published monthly on the Network's website at https:// armedcitizensnetwork.org/our-journal.

Do not mistake information presented in this online publication for legal advice; it is not. The Network strives to assure that information published in this journal is both accurate and useful. Reader, it is your responsibility to consult your own attorney to receive professional assurance that this information and your interpretation or understanding of it is accurate, complete and appropriate with respect to your particular situation.

In addition, material presented in our opinion columns is entirely the opinion of the bylined author and is intended to provoke thought and discussion among readers.

To submit letters and comments about content in the eJournal, please contact editor Gila Hayes by e-mail sent to editor@armedcitizensnetwork.org.

The Armed Citizens' Legal Defense Network, Inc. receives its direction from these corporate officers:

Marty Hayes, President

Gila Hayes, Chief Operating Officer

We welcome your questions and comments about the Network.

Please write to us at info@armedcitizensnetwork.org or PO Box 400, Onalaska, WA 98570 or call us at 888-508-3404.