FCC: FRIEND OR FOE? SDR: TRICK OR TREAT?

J. PIERRE DE VRIES*
SPEECH TRANSCRIPT
GNU RADIO CONFERENCE 2016[1]
BOULDER, COLORADO
SEPTEMBER 15, 2016

* Pierre de Vries is Co-Director of the Spectrum Policy Initiative at the Silicon Flatirons Center for Law, Technology, and Entrepreneurship at the University of Colorado, Boulder. His current work focuses on maximizing the value of radio operation by managing potential and actual interference before and after rulemakings. He is also Visiting Senior Scientist at the Institute for Networked Systems of RWTH Aachen University. He was a Technology Advisor to Harris Wiltshire & Grannis LLP in Washington D.C. (2007–2010) and a Senior Fellow at the Anneberg Center for Communication of the University of Southern California (2006–2007). Previously, he held various positions with Microsoft Corp. in Redmond including Chief of Incubation, and Senior Director of Advanced Technology and Policy. Full biography is available at https://sites.google.com/site/jpdevries/bio [https://perma.cc/9F4M-3FXA].

1. GNU Radio, *GRCon16 – Keynote: FCC, Friend of Foe? SDR, Trick or Treat? Pierre de Vries*, YOUTUBE (Nov. 8, 2016), https://youtu.be/1a8D4aaoS0k [https://perma.cc/88V8-KFB9] [hereinafter *GNU Radio*] (the transcript has been lightly edited for clarity); *See generally GNU Radio Conference 2016*, GNU RADIO, http://gnuradio.org/grcon-2016/schedule/ [https://perma.cc/9RZG-RD2S] (last visited Feb. 26, 2017) (for the GRCon 2016 schedule, including the abstract of this speech).

INTRODUCTION

You could say that the Federal Communications Commission (FCC) is from Mars and Software Defined Radio (SDR) is from Venus. It is still early in their relationship, though, and I'm here this morning to see if we can avoid couples therapy down the road. I'm going to talk about how those two parties relate, how the FCC might look at SDR as a technology, and how the SDR community might want to think about the FCC.

It is a real privilege to be here this morning. Thank you very much to Ben Hilburn for the opportunity to speak with you today.

The intersection between SDR and regulation is something I've been trying to wrap my head around for the last year or so. The question I've been wrestling with is this: is there something to worry about here? I don't know. I am a spectrum guy (a physicist originally), not an SDR guy. I need your help to understand this intersection. I believe that the spectrum policy community in general needs your help too.

In terms of my agenda for this talk, I will first sketch out how FCC decisions and thinking might affect what you do. Next, I will explore what you can do to influence spectrum policy, and how policymakers think. Then I will brainstorm a bit about what you could or should do about that. My goal is to leave about 15 minutes at the end for conversation and discussion—that is probably going to be the most useful and definitely the most fun part of this session.[2]

I. WHY THE SDR COMMUNITY SHOULD WORRY ABOUT REGULATION

The first question is: why should the software radio community—why should you—worry about regulation? In one sense, it's obvious: all non-federal U.S. radio operation must conform to FCC rules. Therefore, how the FCC understands what SDR represents, and its risks, benefits, and threats, is ultimately going to determine what you can legally do with this technology.[3]

The underlying issue is that the promise of SDR is much less visible than the risk. I will give you a bunch of examples in a minute. But first, let's just think about how the FCC affects you.

Perhaps the issue that is most visible to this community is a guideline that the FCC put out in 2014 on the programmability of 5GHz unlicensed devices, including Wi-Fi routers and other non-

2. *Id.* (the discussion begins at https://youtu.be/1a8D4aaoS0k?t=1920) [https://perma.cc/GZG8-KKUM]).

3. I said "FCC," but I know there are a lot of people here from outside the United States. The FCC is what I know best, so I'll talk about FCC proceedings and activities. I believe the dynamics are actually going to be the same in other countries and regions, but the details will be different in different places.

Wi-Fi technologies.[4] This triggered a huge, ongoing debate about whether third party, open source Wi-Fi router firmware like DD-WRT that changes the radio frequency (RF) parameters of radios should be installed by third parties. As I understand it, the open source software development community was very worried that what the FCC proposed to do was going to encourage manufacturers to lock down their routers so that you couldn't use any open source upgrades. That is, you couldn't install DD-WRT, whether or not it affected the RF side of things.

Even the FCC admitted—as the head of the Office of Engineering and Technology, Julie Knapp, blogged at the end of last year—that their guidance "prompted a fair bit of confusion" about whether they were mandating a wholesale blocking of open source firmware modifications.[5] They released a revision that they believed clarified their instructions and goals by narrowly focusing on modifications that can take a device out of compliance.[6] That is, out of compliance with the radio service rules—and those are the kinds of parameters that will keep coming up in this talk. It's typically things like transmission power, or which transmission power and frequency range, out of band emissions, technologies that you need to use in some bands and not in others (such as dynamic frequency selection), and so on.

The FCC's reaction gives one a clue about what they are actually excited about, which is the occurrence of unanticipated, harmful interference from devices that no longer behave the way they did when the FCC last saw them.[7] I'll talk a bit about the Terminal Doppler Weather Radar case in a minute and how it influenced the FCC's thinking.

So, let's back off a bit—what does the FCC actually say about software defined radio? They have been working on this for about 15 years. The first inquiry that I'm aware of was back in 2000.[8] The current rules date from 2005 and require that the "manufacturers [of a software defined radio] must take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio."[9] This software can't allow the user to

4. *Revision of Part 15 of the Comm'n Rules to Permit Unlicensed Nat'l Info. Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Dkt. No. 13-49, First Report & Order, 29 FCC Rcd. 3458 (2014).

5. Julius Knapp, *Clearing the Air on Wi-Fi Software Updates*, FCC: BLOG (Nov. 12, 2015, 12:09 PM), https://www.fcc.gov/news-events/blog/2015/11/12/clearing-air-wi-fi-software-updates [https://perma.cc/CLK9-PHKA].

6. FCC OFFICE OF ENG'G & TECH. LAB. DIV., SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES (2015).

7. In the end, this doesn't seem to have been a problem. *See* Jon Brodkin, *Linksys WRT Routers Won't Block Open Source Firmware*, ARS TECHNICA (May 13, 2016, 7:35 AM), https://arstechnica.com/?post_type=post&p=881369 [https://perma.cc/2XK2-5JYY].

8. *Inquiry Regarding Software Defined Radios*, ET Dkt. No. 00-47, Notice of Inquiry, 15 FCC Rcd. 5505 (2000).

9. 47 C.F.R. § 2.944 (2016).

operate this transmitter out of the FCC approved parameters. Furthermore, and perhaps most importantly, the manufacturer must have what they call "reasonable security measures" to prevent unauthorized modification of the software as it is shipped.[10]

You can see why, with that in the back of their minds since 2005, the FCC was worried when they saw things that were being installed on devices that seemed to change the RF parameters and cause harm.

The other thing that happened more recently is in July 2015 the FCC said, "It's been 10 years. It's probably time to update our rules."[11] And the interesting thing about those rules—the conditions for software defined radios—is that they only apply to devices that are classified as software defined radios and the manufacturer gets to decide if they want to declare their radio to be a software defined radio. Not surprisingly, hardly anybody decided to declare. Who wants extra rules? The FCC is now proposing to incorporate those requirements (for example: software that controls RF parameters) into their general rules, so that they apply to any device that goes through certification by the FCC—you know, when you turn a device upside down and there is an FCC logo on the back that says, "This thing has been certified."[12] All of those devices have to now satisfy these rules about security features, unauthorized changes, and so on.

Now, you hear about these kinds of things, and to me, it sounds really Draconian. It doesn't compute. How can you possibly do all this really great stuff with GNU Radio given all these conditions? There are exemptions![13] The rules don't apply to equipment that is sold as test equipment and the hardware that you are using has been sold as test equipment.[14] Those rules don't apply to USRPS or HackRF or LimeSDR or any of those kinds of things.

Now, I'm not saying there is any indication right now that the FCC is going to remove that exemption for test equipment that would change what you can do with GNU Radio. What you have to think about is: What if the FCC did remove the exemption? Or what if circumstances change? What if there was some hack that frightened Congress, which then said, "Oh my God, the FCC needs to do something about that?" My contention is that this community needs to start thinking about what the regulator might do in those

10. *Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Tech.*, ET Dkt. No. 03-108, Second Memorandum Opinion & Order, 25 FCC Rcd. 1, 587–588, para. 2 (2010).

11. *Amendment of Parts 0, 1, 2, 15, and 18 of the Comm'n's Rules Regarding Authorization of Radiofrequency Equip.*, ET Dkt. No. 15-170, Notice of Proposed Rulemaking, 30 FCC Rcd. 6925, 7726, para. 2 (2015).

12. *Id.* para. 19.

13. 47 C.F.R. § 15.103 (2016).

14. *Id.*

cases.

II. WHY A REGULATOR MIGHT WORRY ABOUT SDR

Why might the regulator worry about SDR? I am going to give a few examples. I am not saying that any of these stories are valid justifications for SDR rules. I am not even saying that SDR is the root cause of the problem, but these are the kinds of things that are what lawyers like to call a "parade of horribles." It is the kind of stuff that could predispose or scare the regulator to make bad rules. I want you to listen to these things not with your own ears, but instead, imagine that you are a policy maker. Imagine you are an FCC Commissioner, or a lawyer, or a political appointee, and you are going to be called up to Capitol Hill to be grilled by Congress if anything goes wrong—if something happens like a plane accident, or somebody is murdered and an SDR was used to disable their home security system. Or imagine that you are an FCC staffer. You are an engineer and you have a profoundly deep knowledge of traditional RF, but you don't know all that much about software and you need to figure out what your boss, a Commissioner, needs to worry about.

A. Example 1: Airport Weather Radar

The first story is about airport weather radar—Terminal Doppler Weather Radar.[15] It is used to detect hazardous wind shear and other climatic conditions that affect planes.[16] Wind shear is a rapid change in wind speed; it tends to occur close to the ground and it is invisible to a pilot.[17] These radars are used at more than 45 major airports in the US, including Denver, to detect wind shear and alert pilots. It's not the biggest risk to aviation, but every year there are five to ten wind shear related accidents, so it's something you should worry about if you fly.[18]

Early in 2009, the Federal Aviation Administration (FAA) became aware of degradation in Terminal Doppler Weather Radar.[19] The operators were seeing noise on their screens. They sent out a team from National Telecommunications and Information Administration (NTIA) Institute for Telecommunications Sciences lab to figure out the problem. This

15. *Terminal Doppler Weather Radar,* NOAA, https://www.ncdc.noaa.gov/data-access/radar-data/tdwr [https://perma.cc/Q4VB-QFNF] (last visited Feb. 13, 2017).

16. *Id.*

17. *See* FED. AVIATION ADMIN.: AVIATION SAFETY INFO. ANALYSIS AND SHARING, WEATHER-RELATED AVIATION ACCIDENT STUDY: 2003–2007 21 (2010).

18. *See id.* at 18; *See also* BOEING, STATISTICAL SUMMARY OF COMMERCIAL JET AIRPLANE ACCIDENTS: WORLDWIDE OPERATIONS 1959–2015 (2015).

19. JOHN E. CARROLL ET AL., CASE STUDY: INVESTIGATION OF INTERFERENCE INTO 5 GHZ WEATHER RADARS FROM UNLICENSED NATIONAL INFORMATION INFRASTRUCTURE DEVICES, PART I (2010).

lab did a lot of work, wrote three reports, and it turns out that the interference was due to U-NII unlicensed transmitters, including Motorola Canopy base stations that were transmitting in this band.[20] The Doppler Radar operates in the U-NII 2 band where there is also unlicensed operations. The way that the radar systems are protected is that unlicensed devices do dynamic frequency selection (DFS), which scans for a radar signature and shuts down if it sees one.

There is a lot of speculation as to why the radar systems did not work the way they should. In at least some of the cases it was related to the software that controlled DFS being disabled. Some of it was because maybe a password got out, or was given out, or because people bought equipment overseas, brought it in, and DFS was switched off. This was a software problem that put aviation at risk.

B. Example 2: GPS Spoofing

The second example is Global Positioning Systems (GPS). Civilian GPS is vulnerable to spoofing and jamming, and that weakness is facilitated by software defined radio. This is worrying because a lot of critical infrastructure depends on GPS—it is not just me using GPS to figure out where I am and where I need to drive. GPS is also used for landing planes and navigating container ships into harbors. Furthermore, the mobile communications standard LTE (Long-Term Evolution) uses very precise timing for which it relies on GPS.

Unfortunately, GPS is a fragile system. In a way, GPS is badly designed. There is a lack of resilience and fallbacks. For example, there is this system called eLoran, which is an upgrade of the old terrestrial navigation system. It is being used in some places now as a fallback for GPS. It is terrestrial, at a higher power, and the signal doesn't come from a satellite. The U.S. started decommissioning its Loran stations in 2010. Fortunately, enough people figured out that this was not a good idea. They have stopped and there has been a recommendation to deploy eLoran in the United States.

Until recently, spoofing GPS used to be the preserve of really sophisticated, well-funded research groups. But at DEF CON 2015, there was a group of Chinese researchers that showed how to spoof GPS using a USRP, HackRF, or BladeRF. Anybody with that equipment could make a big piece of equipment, like a plane or a boat, drive into something that it should not drive into.[21]

---

20. *Id.* at 23.

21. *Spoofing GPS Locations with Low Cost TX SDRS*, RTL-SDR.COM (Sept. 3, 2015), http://www.rtl-sdr.com/spoofing-gps-locations-with-low-cost-tx-sdrs/ [https://perma.cc/V3X9-JPBJ].

Again, if you look at that with your scared glasses on, it looks like a case where a bad actor could cause damage.

C. LTE Jamming

Finally, I want to talk about Long Term Evolution (LTE)[22]. We all depend on LTE, but if we cannot complete a call that is not the end of the world. The trouble is that we are planning to deploy LTE for first responders, paramedics, and fire and police departments.

There was a wonderful paper earlier this year by a team at Virginia Tech that showed attacks on certain protocol subsystems of LTE are very efficient.[23] If you want to jam LTE, the first thing you think about doing is jamming the whole uplink or whole downlink. But if you pick certain packets or certain resource blocks that control the whole thing, you need 20 to 30 dB less power to jam LTE. The paper concluded that LTE is "highly vulnerable to adversarial jamming" and "even the most complex attacks can be easily implemented with widely available open source libraries, low cost software radio hardware with a budget of under $1,500, and basic Linux programming skills."[24] No surprise to any of you, but again, this might lead somebody to worry about SDR and public safety.

There are lots of other examples like breaking into a house with a simple replay attack, or hacking vehicles with wireless key fobs. The new Volkswagens are all vulnerable, and lots of other vehicles are too.[25] My wife bought the Volkswagen Golf. I would like to say, "Honey, don't use the wireless key fob," but she does not have that option. The new Golf does not have a keyhole and owners have to use the wireless.

If you are a policymaker and see stories like these in the news there are two ways to read them. One way is: "This is cool," and I suspect that is how most of us read that kind of thing. The other is: "Oh my God, this is scary." When you hear these stories, you can easily put them in context, right? You understand the caveats as Paul Tilghman was saying yesterday on the panel, essentially that there is a difference between SDR in the lab and SDR in the field.[26]

---

22. *See* Brad Bourque, What's the Difference Between 4G and LTE?, Digital Trends (Dec. 4, 2016, 7:00 AM), http://www.digitaltrends.com/mobile/4g-vs-lte/ [https://perma.cc/QWV3-8PL6].

23. Marc Lichtman et al., *LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation,* IEEE COMMUNIC'NS MAGAZINE, Apr. 2016, at 54–61.

24. *Id.*

25. *See* Andy Greenberg, *A New Wireless Hack Can Unlock 100 Million Volkswagens*, WIRED (Aug. 10, 2016, 4:29 PM), https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/ [https://perma.cc/L23R-PD4Y]; *Bypassing Rolling Code Systems–Codegrabbing/Rolljam*, RTL-SDR.COM (Feb. 8, 2016), http://www.rtl-sdr.com/bypassing-rolling-code-systems-codegrabbing-rolljam/ [https://perma.cc/3JLB-KVRG].

26. GNU Radio, *GRCon16 – Panel: GNU Radio in 10 Years*, YOUTUBE (Oct. 28,

It is hard to take this stuff out to do real things in the world. You also understand that this cool stuff leads to things that people who need to be reelected in November care about. You understand that innovation through SDR creates jobs and creates growth. You understand that highlighting security holes makes people safer. It is the hack that actually leads to the safety. If you do not talk about this stuff, the people in D.C. will only think about the scary things.

III. WHY NOW?

That is the big picture, but why is SDR an issue now? Obviously, we are all increasingly dependent on wireless from airplanes to automobiles; if you've got a VW Golf, you can't avoid wireless for security. But of course, pretty much every nontrivial radio now tunes over multiple bands and is programmable to some extent. It is also a fact that SDR is getting cheaper and the tools are getting better, which means it is easier for people to find the vulnerabilities in old systems that were not designed with this kind of thing in mind. The exploits are easier to execute.

What it boils down to is that SDR undermines some key assumptions that underpin regulations. One is that after the FCC has certified a radio's behavior, it doesn't change. The other is that when you think about threats to critical infrastructure (i.e. GPS spoofing or LTE jamming) only a few very well funded, sophisticated players have access to the technology to do that. No, not true anymore.

IV. HOW THE FCC WORKS

Before I get to how you might link-in with the FCC, I'd like to say a few words about my impression about how the FCC works. What is the game?

Every regulator, and the FCC is no exception, is in the business of making tradeoffs. They need to trade off safety and innovation against economic growth and public welfare. Then they've got the incumbents who are in a band and the new entrants who *want* to be in a band. They must try to find the right balance between all of these.

Think back to the DD-WRT case where there was a question about whether we should allow operational support system upgrades to 5GHz routers. You can read it in two ways. You can say, "We need to do this to prevent interference to weather radar. It was 5GHz unlicensed that affected the radars, so we need to make sure that doesn't happen again by limiting modification." You

2016), https://www.youtube.com/watch?v=XtXLrNEYwBI [https://perma.cc/2FYE-BCCP].

could also look at it the other way, which is the way in which the open source network security researchers argue that improving the security of Wi-Fi devices by making it easy, legally and technically, to keep equipment properly patched is a much greater benefit than the tiny risk that might be posed to airport radar systems.

The other thing that you must bear in mind is that when the FCC is making tradeoffs, they are hearing the best lobbying that money can buy. The arguments on both sides are going to be compelling. One of the things that I found is that I look at an issue and hear the argument and think, "That sounds right to me."

The last, and perhaps most important, thing that we need to bear in mind is that the decision makers in this space are often both lawyers and political appointees. They usually are not engineers. Ultimately, the decisions that they make are on legal and political grounds, not on engineering criteria. For example, there are terms that float around when FCC promulgates regulation such as "harmful interference" which is defined as interference that "severely disrupts, degrades, or repeatedly interrupts." How do I turn *that* into a number? The answer is: you do not. The lawyer gets to interpret that.

Another important thing to bear in mind is that even though people talk about the "U.S. Code," it is not (computer) code. It does not have a single outcome. What you see in the words of a regulation or a statute is not all there is. There is a lot of precedent, custom, and interpretation that goes into how these words are used. That means you shouldn't assume that you will win a regulatory argument by default just because you have the technically more correct position.

V. SUGGESTIONS ABOUT A RELATIONSHIP BETWEEN THE SDR COMMUNITY AND THE FCC

Given all of that, what kind of relationship might you have, you individually or you as a community, with the FCC?

The first thing is to engage with them. Go visit. They love to hear from engineers. They hear from lawyers all the time. They genuinely seek engagement on technical questions. I work with them and maybe I'm biased, but that's definitely been my experience.

Educate them and provide different perspectives. For example, let's go back to that DD-WRT 5GHz router case. You can say things like (and this is what the open source security guys have been saying) "Your concerns should not just be trying to prevent bad people from doing bad things at the RF layer, but there is value in end users being able to fix flaws in these systems. Do not lock everything down. You might prevent an RF problem, but you will inherit a whole raft of problems further up the stack."

You can make arguments such as that risk of interference from the kind of work that happens in this kind of community is tiny, and you will need to set that against the benefits. In fact, it may be that there are risks that are much more severe than SDR hacks. It may be that the real risk is with open source distribution or more likely, one of the cellular operators does a huge upgrade to all of their devices and there is a bug in it that causes an intermittent RF interference problem.

You have the knowledge and understanding to mitigate these risks. You can help the FCC think about them. Typically, when the FCC looks at a problem they get bombarded by the worst-case scenario. The people who feel at risk come along and say, "If you do not stop this, that horrible thing is going to happen." What you need to do, and some of us have been working with the FCC on this (and you can help), is to say, "No, don't do a worst case analysis, do a risk analysis. Don't just look at one hazard, the worst one. Look at all of them. Don't just look at the severity of the hazard; look at the probability. Yes, this hazard might be severe, but it's a one in 10 million chance."

As a community, you can also mitigate the risks for the benefit of the whole. You can (and as a community, you probably should) think through the risks and the responsibilities that you have by working on SDR. I was trained as a physicist. Physicists lost their innocence with the Manhattan Project. The atomic bomb made physicists realize—and this filtered through as I was being trained—that you have to take responsibility for the consequences of the basic research that you do. It has consequences, and ultimately they are on you.

Now, there has not been a Chernobyl or a Three Mile Island or, God help us, a Hiroshima from SDR hacking, and let us hope there never is going to be one. You can help society avoid that. You can make a contribution, and some of you are already doing this. Design radio protocols that are more resistant to adversarial interference. Grow a community of white hat hackers that works with regulators and policymakers to flag the problem. This wireless hacking challenge that Balint Seeber is working on is a wonderful idea. I would love to see more of an intersection between GRcon, DEF CON, and events like that.

I am talking about talking to the FCC. You might say, "My God, go to D.C.! Who do I talk to?" It sounds daunting, I imagine. There are people in this community who are already engaged, who have been engaged for many years. Find them and ask them. If you are in a city where your law school or law schools have a technology law policy clinic, (a clinic is where young lawyers work on real world problems to learn how to do law) ask them for help. Here in Boulder, it is the University of Colorado Law School and Blake Reid runs the

Samuelson-Glushko Technology Law & Policy Clinic.[27]

You have to do that because you need to make a positive case for the stuff you want—because if you don't make your voice heard, you are going to get rules you do not like. After that is done it is really hard to un-bake the cake. It is easier to be in the kitchen while the cooking is going on.

Again, I think about the DD-WRT case. I think the software radio community as a whole has benefitted from the network security researchers who made the case. They provided the counterpoint of this "lock it all down" narrative. That is wonderful and we should be really grateful to them, but it is not going to be sufficient going forward. You can't depend on those kinds of things in the future.

CONCLUSION

So, FCC: friend or foe? SDR: trick or treat?

SDR is a technology, so it is both trick or treat. It depends on how it's used.[28] FCC, friend or foe? Again, it is a false distinction because the answer is neither. You can think about the FCC as being a bit like Ben Hilburn, running GRCon. The FCC is a conference organizer trying to do the best for the whole. It is trying to create an environment where cool things can happen and the hassles are minimized, but it can't please all of the people, all of the time. The other thing is that they work in terms of constraints; in the same way that Ben can't do everything he might want to do here, because of the rules that the venue imposes. The University of Colorado says to Ben, "No, you can't have alcohol in the room at such and such a time." The FCC works under constraints as well. In its case, it is Congress who makes laws that it must fix.

My bottom line is that it would be great if you understood what the FCC worries about and the problems that the agency faces. Help the FCC solve problems, because that is going to help you.

---

27. Even if the clinical faculty cannot engage directly with the project that you are working on, he would be happy to help you figure out how do you file comments, how to schedule a meeting, how to do this kind of stuff, because it is relatively simple for engineers to share their insights. *See Samuelson-Glushko Technology Law & Policy Clinic*, COLORADO LAW, http://www.colorado.edu/law/academics/clinics/technology-law-policy-clinic [https://perma.cc/7QMK-EP9K] (last visited Mar. 25, 2017).

28. *Compare* Sean Gallagher, *This Machine Catches Stringrays: Pwnie Express Demos Cellular Threat Detector*, ARS TECHNICA (Apr. 20, 2015, 3:40 PM), https://arstechnica.com/?post_type=post&p=649761 [https://perma.cc/9PE9-HAW3], *with* Brian Benchoff, *How to Detect and Find Rogue Cell Towers*, HACKDAY (Aug. 9, 2016), http://hackaday.com/2016/08/09/how-to-detect-and-find-rogue-cell-towers/ [https://perma.cc/SS23-ULYH].