# Noirware

**Hal Berghel,** University of Nevada, Las Vegas

*Are we just going to sit here while the unintended consequences of bad design wreak havoc on our lives? A retrospective about RFID creep and GPS abuse is called for.*

No system or software designer, innovator, or inventor has a perfect record. As with baseball sluggers, a 33 percent success rate with significant projects—delivered on time without errors—probably qualifies you as a superstar. So the act of coming up with a bad idea, or a failed implementation thereof, doesn't disqualify you from getting kudos. But there are consumer-level bad ideas and industrial-strength bad ideas. The latter are the more worrisome, especially if they recur with any frequency. As such, I'll deal with them here.

I have drawn an orthogonal distinction between a posteriori bad ideas (those that, in practice, just didn't realize expectations) and a priori bad ideas (those that could or should have been identified as wearing a cloak of dopey by a competent knowledge-domain expert before any work began). Dopey a priori offerings become part of the disaster literature, and many are destined to be featured in eponymous documentaries.

Not everything we *can* do is worth doing. The use of RFID in security-challenging applications is really a poster child for this kind of a priori misguided technology. The last time I discussed this topic,[1] I gave two examples: the use of RFID for keyless entry and transit passes, and the laughable Western Hemisphere Travel Initiative (WHTI) People Access Security Service cards (PASS cards) (https://cdt.org/files/security/20070124passcard.pdf). This WHTI PASS card is a particularly poignant example of how a government's fondness for bad ideas can fill the military–industrial–surveillance–political–media–prison–energy–healthcare–academic–thinktank–corporatist–homeland security complex's coffers.

## TECHNOLOGY ABSURDISM

Well, they're at it again—this time pushing RFID for evidence management (http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8030.pdf). The potential applications that the National Institute of Standards and Technology


0018-9162/15/$31.00 © 2015 IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

(NIST) envisions for this include evidence inventory, chain of custody, in-transit tracking, and access-control management. Nowhere in this 50-page report is there any discussion of security or privacy. This isn't surprising because none of the contributors seem to have any background in security and privacy! This might be another case of the government working with vendors to design products around "insecurity models"—the methodology that gives us yet another act in Bruce Schneier's "security theater."[2]

With RFID evidence management, it's just a matter of time until personally identifiable information (PII) is leaked, the chain of custody is found by a court to be corrupted, or some RFID source or other is spoofed to provide unauthorized access to sensitive information. I'll repeat my mantra: RF doesn't obey property lines and isn't a good candidate for security- and privacy-challenging applications—especially when it's built around a weak security model. We need to wrap our heads around this concept!

RFID for keyless entry and pass cards are examples of *technology absurdism*: technology development that ignores, fails to appreciate, or underrepresents obvious negative externalities. Placing technology development in the hands of the unskilled, ill-trained, or poorly supervised pretty much guarantees that the resulting technology will fail to meet our needs and expectations and expose us to increased risk. Those of you who are software engineers and developers could write books about this phenomenon from your own personal experiences. It's incumbent on all of us to remember that many, if not most, of the worst technological ideas were identifiable as such a priori. In the hands of bad leadership, technological absurdism drifts toward technology nihilism that in turn drives subprime innovation of limited or ephemeral value. The National Security Agency (NSA) dragnet surveillance programs typify technological nihilism in this sense, and they're linked to exceedingly poor leadership (see my column, "Leadership Failures at the National Security Complex"[3]).

## INTRUSIONS ON HERTZIAN SPACE

I want to single out two really clever innovators who are addressing these issues: Limor Fried and Todd Humphreys. Following Anthony Dunne and Fiona Raby,[4] Fried suggests that *design noir* might be used as an antidote to electronic devices that fail to peacefully inhabit *Hertzian space*—the space shared by humans and their devices.[5] This is an exceedingly clever and informative way to approach the problem of technological subterfuge undermining an individual's privacy—including the NSA's surveillance programs, hacking into the Global System for Mobile Communications (GSM) cellphone infrastructure,[6] and warrantless wiretaps.

> Remember that many, if not most, of the worst technological ideas were identifiable as such a priori.

As an aside, it's worth noting that many of the NSA's secret codenames—AURORAGOLD, PRISM, XKeyscore, MUSCULAR, Stellarwind, CO-TRAVELER, Bullrun, EvilOlive—have been so widely discussed and discredited that they've entered the public lexicon. For those of you who want to know more, the Electronic Frontier Foundation (EFF) offers an excellent NSA Domestic Spying Timeline (www.eff.org/nsa-spying/timeline). EFF deputy general counsel Kurt Opsahl (see his video at www.eff.org/nsa-spying/how-it-works) draws our attention to the fact that EvilOlive is both a palindrome and an anagram, and its use justifies the special sobriquet of its devilishly clever codename.

According to Fried, electromagnetic propagation in the form of visible light, radio waves, x-rays, and the like has the potential to affect us in subtle and multifarious ways. Perceptible radiation, such as acoustics and other stimuli that affect our senses, is much easier to deal with and far less insidious than imperceptible radiation because we're continuously reminded of its presence. Such antisocial impositions on our privacy are easily identified as personally irritating, intrusive, unwanted, and sensory-overloading. Overheard cellphone conversations, ubiquitous television chatter in public spaces, elevator music, and boom boxes fall into this category. (My personal feeling is that body odor, tracking cookies, the smell of mint, and most of the NSA's surveillance programs should be included as well!) Fried argues that design practices ought to factor these in with technical specifications and manufacturing costs. This is a convincing argument that's worthy of serious consideration.

Fried sees a need to develop countertechnologies to thwart these insidious intrusions—antidotes to "nullify the invasion." She observes that this fits within a Marshall McLuhan–esque natural technology/anti-technology order of things.[7] She proposes "that designers, technologists, and artists should ... come up with new ideas for

how the consumer may defend his or her personal space from unwanted electronic intrusion."[5] What a notable goal! The problem is that the aforementioned complex will use every legal and political tool at its disposal to prevent that strategy from succeeding. This is a David-versus-Goliath situation if ever there was one.

## NOIRWARE

Fried also looks at electronics with insidious side effects that aren't fully disclosed to the consumer. Examples include cellphones that can be remotely controlled by the carrier to turn on the microphone and camera without the user's knowledge or permission[8] and the recent spate of International Mobile Subscriber Identity (IMSI)-catching activity, where fake cellphone towers intercept phone traffic and track users' whereabouts.[9] The fact that cellphones could be used as "roving bugs" or PII repositories by law enforcement, the surveillance state, common carriers, cyber-weapon mercenaries, and hackers is one of those "added features" that vendors, carriers, government agencies, and nongovernment organizations (NGOs) try to conceal. Fried argues for innovation that enhances the user's control of existing products beyond the means provided by the manufacturer, or innovation that could actually subvert the product's intended use. Her suggestions anticipated Edward Snowden's revelations by several years.

I want to build on Fried's worthy goals. I'll use the term *noirware* to mean any disruptive technology that limits or neutralizes those unadvertised or unintended uses of a product that are inconsistent with the user's expectations of security and privacy. Note that the emphasis is on the user's expectations, not the advertised features. Now that we live in the era of amorphous product disclosures that may or may not be accurate, complete, or reliable, this distinction is important. Historically, software shipped without warranty expressed or implied. These days, we can't be certain that a product ships without back doors, malware, faulty encryption, or even known deficiencies that are shared with those who want to surveil us.[10] It's worth remembering that Snowden's NSA PRISM program revelations showed that it had retrieved data from US high-tech firms without court orders.[11]

Further extending our working definition, we must distinguish between offensive and defensive noirware. The greatest barrier to successful noirware deployment is that current technology rarely allows a purely defensive strategy. In most cases, noirware would be an adversarial technology that is difficult to control as it nullifies rather than neutralizes electromagnetic energy.

Consider Fried's Wave Bubble (WB; www.ladyada.net/make/wavebubble/index.html). WB creates a low-energy 2-meter diameter "cloud" of RF noise that targets the usable frequencies of the offending device—it's a perfect antidote to the imposition of other peoples' one-sided cellphone calls on your personal auditory happy space. (See Fried's 2007 Gadgetoff presentation at www.youtube.com/watch?v=Oesez3A-Tqg.) While the concept is great, it runs afoul of US federal laws that make intentional RF jamming by private citizens illegal. In fact, in the US it's even illegal to advertise the sale of RF jammers,[12] though the technique is apparently popular with some foreign faith leaders.[13]

I'd be remiss if I failed to comment on the Federal Communication Commission's (FCC's) approach to jammer regulation, which is both technologically naive and overreaching. For one, the jamming ban applies to any RF source, even when that source is an illegal one used to eavesdrop without court authorization—a paradigmatic Fourth Amendment violation. On my reading, using a low-energy jammer to jam a cellphone in your own backyard to prevent invasive eavesdropping through remotely turning on the phone's microphone and camera, you—not the eavesdropper—would be subject to prosecution.[14] Of course, there are good reasons to prevent reckless and irresponsible RF jamming. A recent case involved a truck driver who jammed his mobile GPS, in turn blocking a new GPS system to be used by the Newark airport air-traffic control system.[15,16] This isn't a good argument against active RF personal privacy defense systems as such and in general, but rather an argument against irresponsible deployment. To ban all jamming in all contexts while allowing RF interception and surveillance throws the proverbial RF baby out with the digital bathwater. It's simply unreasonable to allow the use of RF tracking devices and at the same time block any active defense measure. No one can live in mobile Faraday cages.

Although Fried's WB technology might not be ready for prime time, the spirit and enthusiasm behind it is worthy of continued investigation. It's entirely possible that WB v2.0, together with a more reasonable approach to FCC regulation, could converge on the next digital aspirin to relieve RF tension and stress. We welcome Fried and her colleagues to this challenge.

Not everything we *can* do is worth doing.

## GPS AND LORAN-E

Our next candidate for technological absurdism is GPS—at least as it's currently implemented for public and commercial use. This brings us to our second worthy innovator, Todd Humphreys, who performed the best analysis that I know of regarding the deficiencies of GPS[17] (with corresponding TED video[18]). He's been in the news a lot since demonstrating how easy it

is to capture control of GPS-based automated marine navigation systems with GPS spoofing.[19] Like Fried, Humphreys should be commended for a yeoman effort in exposing technological hubris and a priori design flaws.

GPS, like RFID, is a useful technology in most manifestations—and both were developed with little serious concern for security. In the earliest common commercial applications, neither employed robust encryption or authentication protocols. They were as wide open as early Wi-Fi. That's actually not a bad analogy, because the initial authentication and encryption protocol for 802.11 (Wired Equivalent Privacy, or WEP) was just as lame as the initial encryption algorithm for RFID that was built into the classic MIFARE chip[20] (this video explanation is especially illuminating: http://media.ccc.de/browse/congress/2007/24c3-2378-en-mifare_security.html#video). All three systems exemplify technology hubris or, to repurpose computer scientist Edsger Dijkstra's words, mistakes carried through to perfection. To my knowledge, commercial GPS still doesn't offer support for encryption or authentication. Based on the Iranian capture of RQ-170 Sentinel drone,[21] it appears that even hardened military GPS guidance might be vulnerable to basic RF jamming attacks and GPS hacks. This shouldn't come as a surprise to anyone.

## STANDARD GPS

Basic GPS operation goes roughly like this: satellite almanac and position data are retrieved and stored in the GPS receiver as it locks onto the signals. Commercial GPS uses code-phase tracking that triangulates the position from four or more of the several dozen satellites in medium Earth orbit (approximately 12,000 miles above Earth), all of which are controlled and synchronized from ground stations. Unique 1,023-bit sequences (Gold codes) individuate the satellites. The satellite signals are sent on a roughly 1,500-MHz carrier frequency, which allows the Gold codes to be repeated at millisecond intervals. The GPS receiver then synchronizes the broadcast Gold code with a stored copy of the code. The offset required to match sequences determines the time delay, from which the distance from the satellite may be calculated. Since President Clinton shut off Selective Availability (SA)—intentional signal-hobbling to reduce accuracy for national security purposes—commercial GPS has had an accuracy of a few meters. SA was one form of bias error. Clock errors, satellite position errors, weather-induced signal errors, and multipath (reflection) errors can also produce position anomalies of several meters. But the granddaddy of GPS errors is what geographer Peter Dana calls a "blunder."[22] GPS blunders can introduce errors so large (sometimes many miles) as to render GPS unusable.

Humphreys' GPS spoofer is a utility that can produce blunders. He has successfully demonstrated how it can introduce dangerous navigational errors in aircraft and marine applications. This shows that absent a robust security model, commercial GPS is currently untrustworthy with no antidote on the horizon. Commercial GPS is an example of an RF application for which Fried's WB technology wouldn't help us because there's no way to jam the device without eliminating functionality. But there's more. Humphreys points out that GPS dots[17]—little GPS trackers that measure less than a centimeter on a side—are catching up with RFID tags in popularity. Combined with GPS, carrier-phase tracking is far more accurate than code-phase tracking, because it links the location to 1 percent of the wavelength of the carrier frequency, or about 2 millimeters. For this, the only countermeasure could be large quantities of micro-WBs (let's call them *bubblettes*), but of course this requires that you find the GPS dots before you can neutralize them.

## FAILURE PORN

Both Fried and Humphreys provide considerable insight into the negative externalities associated with modern technology. But in so many of these cases, the problems were known from the start by domain experts. RFID technology dates back at least as far as inventor Léon Theremin's listening device "The Thing" that was planted in Ambassador W. Averell Harriman's Moscow residence in 1945. Viable transponders were in use decades before that, and GPS technology dates back to the late 1950s. Does it seem reasonable that for the past 60-plus years no one asked what would happen if RFID and GPS were subjected to out-of-band applications? They're no different than children's toys with sharp edges, Takata automobile airbag inflators that have the potential to blast passengers with shards of steel,[23] drones that can be remotely hijacked using techniques similar to those described by Humphreys,[24] insecure webcam/baby monitor systems,[25] or the glitzy new home automation systems that invite intrusion and compromise.[26]

> Let's insist that potential technology abuse be included in the calculated velocity of all innovation.

These are but a few technologies in use that were and are really bad ideas. It's time to insist that potential technology abuse be included in the calculated velocity of all innovation, or else we, as consumers, should refuse to buy or use it. Apropos of viticulturist Paul Masson, the mantra should be: we will see no technology shoveled before its time. And don't assume that

corporate-financed politicians will protect us in this regard; for the most part, they're conversely incentivized.

What produces these poorly thought-through technologies that are unfit for public consumption? It's related to what venture capitalist Geoff Lewis calls "failure porn"—the adulterated and adorned view of failure packaged for mass consumption.[27] Failure porn and the hazardous technologies discussed above exist within interrelated dystopic frameworks, both of which follow from a culture of unreflective, feckless design, irresponsible development, and churlish marketing.

Finally, on 28 December 2014, Karsten Nohl of Security Research Labs announced a new application for rooted Android 4.1 or newer cellphones called SnoopSnitch that monitors a spectrum of Signalling System 7 (SS7) cellphone protocol vulnerabilities (including interception attacks like IMSI-catching and re-routing attacks) at the 31st Chaos Computer Conference (www.youtube.com/watch?v=lQ0I5tl0YLY). Nohl observed that SS7 could be secured if the carriers would just commit to reasonable customer privacy standards. Failing that, no 3G GSM network should be assumed secure, especially since the 64-bit A5/3 cipher has been broken. Additional information is available online at https://gsmmap.org/assets/pdfs/gsmmap.org-country_report-Germany-2013-12.pdf.

Limor Fried and Todd Humphreys have done the heavy lifting for us. They've exposed a new suite of bad ideas that were not carefully or completely thought through before deployment. It remains for the rest of us to resist the shoveling of immature technology. Think Paul Masson!

## REFERENCES


1. H. Berghel, "RFIDiocy: It's Déjà vu All Over Again," *Computer*, vol. 46, no. 1, 2013, pp. 89–92.
2. B. Schneier, "Beyond Security Theater," *New Internationalist*, 1 Nov. 2009; http://newint.org/features/2009/11/01/security.
3. H. Berghel, "Leadership Failures at the National Security Complex," *Computer*, vol. 47, no. 6, 2014, p. 64-67.
4. A. Dunne and F. Raby, *Design Noir: The Secret Life of Electronic Objects*, Birkhauser, 2002.
5. L. Fried, "Social Defense Mechanisms: Tools for Reclaiming Our Personal Space," master's thesis, Dept. of Electrical Eng. and Computer Science, MIT, 2005; www.ladyada.net/media/pub/thesis.pdf.
6. R. Gallagher, "Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide," *The Intercept*, 4 Dec. 2014; https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones.
7. M. McLuhan, *Understanding Media: The Extensions of Man*, The MIT Press, 1994.
8. D. McCullagh and A. Broache, "FBI Taps Cell Phone Mic as Eavesdropping Tool," *CNET News*, 1 Dec. 2006; http://news.cnet.com/FBI-taps-cell-phone-mic-as-eavesdropping-tool/2100-1029_3-6140191.html.
9. H. Fakhoury, "Stingrays Go Mainstream: 014 in Review," Electronic Frontier Foundation, 2 Jan. 2015; www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream.
10. J. Menn, "Exclusive: NSA Infiltrated RSA Security More Deeply Than Thought—Study," Reuters, 31 Mar. 2014; www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331.
11. B. Gellman and A. Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *The Washington Post*, 20 Oct. 2013; www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.
12. "Consumer Alert: Using or Importing Jammers Is Illegal," DA 12-347, Federal Communications Commission, 6 Mar. 2012; www.fcc.gov/document/consumer-alert-using-or-importing-jammers-illegal.
13. Z. Mintz, "Italian Priest Blocks Cell Phone Signals at Church," *International Business Times*, 18 Dec. 2014; www.ibtimes.com/italian-priest-blocks-cell-phone-signals-church-1762826.
14. "Jammer Enforcement," announcement, Federal Communications Commission, www.fcc.gov/encyclopedia/jammer-enforcement.
15. C. Matyszczyk, "Truck Driver Has GPS Jammer, Accidentally Jams Newark Airport," *CNET News*, 11 Aug. 2013; www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport.
16. J.C. Grabowski, "Personal Privacy Jammers: Locating Jersey PPDs Jamming GBAS Safety-of-Life Signals," *GPS World*, 1 April 2012; http://gpsworld.com/personal-privacy-jammers-12837.
17. T. Humphreys, "The GPS Dot and Its Discontents: Privacy vs. GNSS Integrity," *Inside GNSS*, Mar./April 2012; www.insidegnss.com/auto/marapr12-Humphreys.pdf.
18. T. Humphreys, "How to Fool a GPS," video, TEDxAustin, Feb. 2012; www.ted.com/talks/todd_humphreys_how_to_fool_a_gps#t-891640.
19. B. Dodson, "University of Texas Team Takes Control of a Yacht by Spoofing its GPS," *Gizmag*, 11 Aug. 2013; www.gizmag.com/gps-spoofing-yacht-control/28644.
20. M. Morbitzer, "The MIFARE Hack," Proxmark.org; www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20Classic/The_MIFARE_Hack.pdf.
21. S. Peterson, "Downed US Drone: How Iran Caught the 'Beast,'" *The Christian Science Monitor*, 9 Dec. 2011; www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.
22. P.H. Dana, "Unit 017: Global Positioning System Overview," *The NCGIA*

*Core Curriculum in GIScience*, revised 7 July 2000; www.ncgia.ucsb.edu/giscc/units/u017/u017.html.
23. H. Tabuchi, "Takata Saw and Hid Risk in Airbags in 2004, Former Workers Say," *The New York Times*, 6 Nov. 2014; www.nytimes.com/2014/11/07/business/airbag-maker-takata-is-said-to-have-conducted-secret-tests.html?_r=1.
24. A. Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible," *Wired*, 16 Dec. 2011; www.wired.com/2011/12/iran-drone-hack-gps.
25. "Peeping into 73,000 Unsecured Security Cameras Thanks to Default Passwords," *Network World*, 6 Nov. 2014; www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html. [written under alias]
26. T. Renzenbrink, "30C3: Hacks Demonstrate Insecurity of Home Automation Devices," *Tech the Future*, 10 Jan. 2014; www.techthefuture.com/technology/30c3-hacks-demonstrate-insecurity-of-home-automation-devices.
27. G. Lewis, "Failure Porn: There's Too Much Celebration of Failure and Too Little Fear," *The Washington Post*, 4 Dec. 2014; www.washingtonpost.com/opinions/failure-porn-theres-too-much-celebration-of-failure-and-too-little-fear/2014/12/04/6bc15816-73ec-11e4-a5b2-e1217af6b33d_story.html. ftp://ieeecs:@ftp.computer.org/House_Ads/Ads%204C/PDFs/cps_mobile_app_3qtr_mjb_v2.pdf.

**HAL BERGHEL** is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.