Legislating Technology (Badly)

Hal Berghel, University of Nevada, Las Vegas

It's characteristic of willfully uninformed politicians to react to crime with legislative quick fixes when common sense dictates otherwise. Nowhere is this more evident than in legislation affecting technology and innovation.

Due to the computational power of underlying platforms, digital kill switches have a much broader capability and use than earlier industrial panic switches. In the case of mobile computing devices and smartphones, the purpose of the kill switch is to make theft unattractive. Protections include "wiping" the data off the device and/or "bricking" the device so that it is unusable. Consumer Reports estimated that in 2012 there were 1.6 million victims of smartphone theft.[1]. Add to that the fact that "Apple, Google, Microsoft, and Samsung—plus Motorola, which is owned by Google—control 90 percent of the US smartphone market," so there aren't many manufacturers involved.[2]

STAKEHOLDERS

There are a variety of proposed statutory protections to discourage mobile device theft. One good source of information on this issue is the City and County of San Francisco District Attorney's Secure Our Smartphones Initiative (www.sfdistrictattorney.org/index.aspx?page=263). California introduced recent kill-switch legislation in late January 2014,[3,4] followed closely by the US Senate bill 2032.[5] Similar legislation has been proposed in the House of Representatives and in state legislatures under the general rubric of Smartphone Theft Prevention Acts. We shall investigate whether and to what degree such legislation is likely to be effective, and whether negative consequences might be anticipated.

0018-9162/15/$31.00 © 2015 IEEE

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

Let's begin by analyzing the incentives behind various stakeholder positions.

Incentives against passage

Obviously, a petty thief will oppose a kill-switch bill that requires bricking as that would make profitable resale of a stolen device unlikely. In addition, an identity thief wouldn't welcome a "data wipe" feature. Note how even thieves' incentives are subtly different: the petty thief wants a usable device, whereas the identity thief wants usable data. The petty thief is motivated by resale prices. Some news sources claim that the better smartphones can be resold for up to US$1,200 each in the Pacific Rim and Africa.[2] So if such legislation were to pass, expect a cottage industry to arise selling lead sleeves to shield mobile devices from kill-switch activation as thieves cart away their booty. The identity thief, however, has little concern about the device's usability as long as the data can be copied.

The telecommunications industry and carriers have no incentive to pass this legislation—so long as there's continued use of their product—regardless of registered owner or original source—they'll continue to profit from the subscription service. The devices are the mere vehicles through which they sell their service. In this case, the carriers' incentive is aligned with the petty thief—that is, to keep the device usable. A secondary benefit is that the registered user is on the hook for the subscription fees and charges until the phone's service is suspended.

Strong opposition from the technology sector—which opposes regulation on principle—should also be expected. There's some sense to this position, because a sufficiently robust mobile-platform encryption regimen should protect personally identifiable information (PII) from unauthorized users, which might satisfy most users' privacy needs. Vendors might also feel that regulation with penalties restricts free trade. Simply put, they bear no burden for theft and loss.

The Wireless Association (CTIA) articulates the manufacturers' and vendors' position, which is that it's obviously bad public policy for states to regulate products that are sold internationally. They prefer owner-based initiatives involving downloadable apps together with vendor-optional databases that would prevent domestic use of stolen phones.[6] However, they have no problem with legislation that penalizes users who reprogram phones—whether stolen or not.

Manufacturer and vendor incentives converge around protecting unimpeded business practices. Their interests differ when it comes to mandated standards for the mobile device itself. Mandated kill-switch legislation requires manufacturers to rework their mobile platforms. Of course, if the California legislation takes root in a few larger states, this issue will become moot as manufacturers will find it less expensive to change their entire product line to satisfy California regulators, and then just not activate it in non-requiring states. It should be noted that manufacturers eventually removed their opposition to the California kill-switch bill, but some technology companies like Google and Microsoft will require users to opt in to theft prevention services.[7]

Incentives for passage

Some stakeholder communities support kill-switch legislation. For one, the typical mobile device owner might appreciate the ability to protect their PII via remote wipe. They might also perceive a benefit from bricking the phone to discourage petty thievery and prevent unauthorized use. Thus, from the user's point of view, opt-in kill switches might be perceived as public good. This naive view is shared by the majority of politicians.

> Not all criminals are opposed to kill switches on mobile devices: major crime lords and terrorists could actually benefit from them.

Why is this naive? Consider the interests of the hacker, criminal, and terrorist communities. Here we have an entirely new mobile platform attack vector that functions in much the same way that ransomware (such as CryptoLocker and FBI Moneypack) does at the workstation and notebook levels. Further, what major criminal wouldn't benefit from a kill switch with wiping and bricking capabilities as a way of thwarting law enforcement evidence collection and surveillance? On this account, the criminal or terrorist is incentivized to develop a network capable of remotely wiping and bricking mobile devices that have been, or are about to be, seized by law enforcement agencies.

Conversely, there are two complexities. From the software epidemiology point of view, the technology (code) that allows data wiping shares DNA with the technology (code) that would be used to offload the PII to another platform by networking, Bluetooth, or direct connectivity. This would incentivize government intelligence and surveillance agencies to develop such hacks for remote deployment.[8] The only chance of preventing this kind of infiltration would be to deploy robust

encryption with open source software on mobile platforms. If you're a criminal, the logical next step is to brick the phone so that a potential victim is denied access to protective services.

Neutral

Finally, there's the neutral position toward the legislation. Although some carriers might fall into this category, the mobile platform insurance carrier seems to be the most natural fit. Cell phone insurance premiums are estimated to produce US$8 billion per year in revenue for carriers in addition to approximately US$200 billion in revenue for the wireless service.[9] This insurance has become what *Warranty Week* calls a "monster hit" for the estimated 150 million domestic smartphones in use—100 million of which are insured against loss. With mandated kill switches, insurance carriers' risk would remain primarily device replacement. Though their premium/risk ratios might change, we would expect that their revenue would remain constant.

So there you have it: the good, the bad, and the ugly of proposed kill-switch legislation. The operative question is whether reasonable, purposeful legislation will result from such conflicting motives and mixed incentives. The interplay between interests is exceedingly subtle and likely beyond the politicians' capacity to appreciate as they tend to lack capacity to appreciate nuance. And don't forget lobbying efforts in support of the political donor classes—any forthcoming kill-switch legislation would have a low expected yield rate in terms of public good. You might find the landscape described above useful in interpreting proposed federal legislation.[5]

SCREEN DOOR ENCRYPTION

Encryption has always been the darling of bureaucrats and tyrants. The earliest bureaucratic interference that I recall came from the National Security Agency (NSA) in the early 1980s when its former director Bobby Inman tried to coopt ACM and IEEE conferences by insisting on pre-publication censorship for all scholarly papers involving cryptography.[10] A committee of representatives from the professional societies (including ACM, the Computer Society, and IEEE) that publish cryptographic research reached a compromise by encouraging voluntary self-censorship. The only dissenting vote came from Computer Society representative George Davida who correctly predicted that such incursions into the academy could undercut First Amendment protections and ultimately subvert scholarship. History has confirmed Davida's predictions.

> The naive view of kill-switch legislation is too crude to address the subtle interplay between stakeholder interests.

Not to be thwarted by academic freedom arguments, big government made another assault on computing research when it attempted to prosecute PGP (Pretty Good Privacy) inventor Phil Zimmerman for alleged Arms Export Control Act violations in the early 1990s.[11] The persecution was apparently even extended to those who wrote op-ed pieces about Zimmerman's plight in Bay Area newspapers.[12] Nothing so offends authoritarians as the thought that someone might speak ill of them behind their backs.

The latest attack on encrypted communication came this past summer from FBI director James Comey, who relied on the surveillance-state national security mantra to motivate Congress to require that all strong encryption systems have a backdoor for the FBI.[13] Apparently, Comey finds Apple and Google particularly irritating for steadfastly refusing to voluntarily comply with FBI requests to share their customers' private information (at least after being outed by Edward Snowden for doing just that). Comey speculated before the Senate Intelligence Committee that inserting a special tiny little backdoor just for the FBI that could not possibly be exploited by others shouldn't be much of a technological challenge. As he sees it, computer scientists just haven't been properly incentivized ("extraordinary incentivization"?). The 8 July 2015 congressional hearings illustrate his opinions on this.[14]

Comey's presentation to the Brookings Institution on 16 October 2014 provides a clearer statement of his opinion:[15]

> *Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.*

As the Church Committee's revelations of COINTELPRO showed, the FBI has a long history of highly questionable surveillance, wiretaps, and sundry black bag operations against US citizens—including sending suicide notes to Martin Luther King, Jr.[16] Recently, it's become fashionable for the FBI to use National Security Letters (NSLs) and "exigent letters" to spy on citizens and journalists,[17] while claiming that this is done under the watchful eye of a "secret" oversight regime. (For more on NSLs, see the Electronic Frontier Foundation's (EFF's) National Security Letter Timeline [www.eff

.org/issues/national-security-letters/timeline].) So, while Comey's concern is that the bad guys might "go dark," many citizens are concerned that the FBI might "go rogue." It's axiomatic that when civil libertarians feel it's no longer possible to ensure that the government operates within the law, any government request for increased surveillance powers is likely to be strongly opposed.

What's more surprising is that even Comey's peers don't agree with him. In a recent op-ed in *The Washington Post*, Mike McConnell, Michael Chertoff, and William Lynn argue that the sort of secure communication that Comey objects to is in fact for the greater public good because it protects information from exploitation:[18] "The result will be to expose business, political, and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process."

But that's a criticism based on political realities. A more pointed criticism is based on the technology itself. Independent reporters have weighed in on this in near unison. The Center for Democracy and Technology had this to say: "Any backdoor the government can walk through to uncover evidence will eventually be used by malicious actors to exploit our personal information."[19] Encryption makes us safer.

The Intercept goes further in debunking the FBI's claims that encryption interferes with effective prosecution of criminals.[20] When asked to provide specific examples of crimes that had been averted due to phone data that might be encrypted in the future, Comey offered the following variation on the surveillance-state mantra:

> *Rescuing someone before they're harmed? Someone in the trunk of a car or something? I don't think I know—yet? I've asked my folks just to canvas—I've asked our state and local partners are there some examples where this—I think I see enough, but I don't think I've found that one yet. I'm not looking. Here's the thing. When I was preparing the speech, one of the things I was inclined to talk about was—to avoid those kids of sort of "edge" cases because I'm not looking to frighten people. Logic tells me there're going to be cases just like that, but the theory of the case is the main bulk of law enforcement activity. But that said I don't know the answer. I haven't found one yet.*[20]

Cutting through the doublespeak, Comey is saying that he has no such examples. He has since taken his fear mongering global, with unspecified and undocumented ISIS threats.[21]

But by far the most important argument against government back doors, front doors, or screen doors for that matter, to encrypted communication comes from the encryption experts themselves. On 6 July 2015, some of the most famous computer scientists in the field wrote the definitive rejection of Comey's backdoor program entitled "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications."[22] The report shows that the FBI proposal would overturn best practices like forward secrecy, make the systems more complicated than they need to be, and invite all manner of criminals, terrorists, and nation-state aggressors to find and exploit loopholes. That's top-drawer policy! And yet, amidst these conflicting motives, bureaucratic hubris, and ideological hyperbole, Congress pushes on with their attempt to draft the perfect piece of legislation while the special interests cheer them on from the sidelines.

911-SWATTING

My final example of legislative ambitions gone awry deals with the efforts to protect the 911 emergency response system. The 911 phone dispatch system works by routing 911 voice signals along with call information (like phone number, mobile phone GPS coordinates, GPS coordinates based on service provider triangulation, and so on) to a proximate dispatcher, who then relays the essential information (possibly augmented by proprietary data from the service provider or dispatcher), to the responders. The situation is similar with VoIP except that the Internet is the carrier rather than the telecom. All signals are digital, so there are several attack vectors available to hackers.

Christian Dameff and his colleagues discussed in a DEF CON 22 video[23] three goals of hacking into the emergency 911 phone system: to initiate inappropriate 911 responses, to interfere with legitimate responses, and to monitor the 911 system for opportunistic insights. From the hacker's perspective, all three goals may be subsumed into one since they only differ by intent. If you're unfamiliar with the 911 system, viewing this DEF CON 22 video is time well spent.

Hacking techniques like spoofing IDs (at either the mobile or network levels), SQL injection, denial-of-service attacks, and IMSI (International Mobile Subscriber Identity) catching all suggest themselves. Modern cellular systems render caller ID spoofing moot since the service provider largely ignores handset phone numbers in lieu of internal firmware IDs so anonymizers like SpoofCards aren't consistently reliable in this application.

From the software epidemiology point of view, the technology (code) that allows data wiping shares DNA with the technology (code) that would be used to steal the data.

The same can be said of location-spoofing apps for mobile devices—the provider might be using signal triangulation rather than reported coordinates. But spoofing can still result at the level of tower communications by a determined aggressor with sufficient technical capability and an understanding of the protocols involved. Remember that all cellular traffic, including authentication, is RF, and RF doesn't obey property lines. The point is that you can't rely on mobile device reports when the attacker has an appropriately configured computer and RF transceiver. In addition, 911 communications remain largely unencrypted, so the referent IDs, GPS location data, tower and carrier IDs, and so forth could be transmitted in clear text—an invitation for hackers. Add to this the proliferation of carrier- and dispatcher-side databases that might not be well secured. Finally, there is Dual-Tone Multi-Frequency (DTMF) baiting, as many dispatchers redirect calls and the tones can be recorded and the numbers recovered from tone extractors, thus giving hackers access to undisclosed, internal communications links. Most intriguing of all is the VoIP exploitation potential, which opens the 911 system to a full range of Internet hacks, anonymizers like TOR, and a potpourri of other exploits using burner phones. In other words, the 911 dispatch system is rife with well known and well understood security and privacy problems.

Let's look at the case of eliciting inappropriate 911 responses; this hack du jour is called "swatting" and involves reporting bogus life-threatening situations—terrorist threats, kidnapping reports, hostage situations, and so on—to a 911 dispatcher. The goal of this criminal mischief is to spur local SWAT or tactical law enforcement units into a response to the bogus threat—hence the term. If the goal is to intimidate, interrupt, or embarrass a public figure, it's called "celebrity swatting." If the target is someone who wronged you, it's called "revenge swatting." If the target is an airport, it's called "fly swatting," and so forth.

> Big government's solutions to computing crimes are reactive and retributive—rather than solving problems at the source.

The recent California Assembly bill AB47 (2013) is a typical government reaction to a technology crime trend (www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0001-0050/ab_47_cfa_20130415_101427_asm_comm.html). Whereas existing California law made misuse of the 911 service a misdemeanor that carried fines, AB47 seeks to deal with "malicious and dangerous swatting calls" by upping the fines to a minimum of US$10,000. Michigan has an even more onerous law that adds a 4- to 15-year prison term to the same level of fine, depending on whether someone was injured or killed as a result of the call (www.legislature.mi.gov/documents/2011-2012/billanalysis/house/pdf/2011-HLA-5431-3.PDF). Not to be outdone, the US House of Representatives proposed the Anti-Swatting Act of 2015, HR 2031 (www.govtrack.us/congress/bills/114/hr2031/text), which seeks to amend the Communications Act of 1934 to provide penalties of 5–20 years and reimbursement of the full cost of responding.

These big-and-powerful government responses might appeal to authoritarians, but they're ineffective. In addition, consider the social consequences. Who are these swatters? Is incarceration for 5–20 years in a federal prison an appropriate sentence for a script kiddie with a grudge? Or an obsessive fan? The people who do these things are deranged; what they need is psychological help, not a scholarship to crime school. And, the possibility of resulting injury would diminish if law enforcement would take a swerve around responding to 911 calls like Normandy invasions. Maybe we should return to the "protect and serve" mission rather than "overpower and subdue." In one recent study by the Utah legislature, 65 percent of the SWAT and tactical team assaults were forced-entry raids to serve warrants, without giving the occupants an opportunity to answer the door. Ah, yes, I hear you cry, but given advanced warning the occupants would have opened fire on the police. Apparently not, because weapons were found on the scene in less than half a percent of the cases (http://libertasutah.org/drop/sb185_2014.pdf).

Without question, the primary cause of swatting and other 911 vulnerabilities is an immature approach to infrastructure security, and for that the blame lies squarely with the telecoms, service providers, and public service agencies. Big government's solutions to computing crimes are reactive—retribution after the fact—rather than solving problems at the source. Swatting can be reduced, if not eliminated, by implementing simple, well-understood best practices: robust encryption at all system levels; the use of secure TCP/IP communication; and avoidance of all security-through-obscurity tactics, such as the use of unregistered phone numbers for internal dispatcher communications, and so on. Dwelling on punishing offenders is misguided, wasteful, and counterproductive.

If legislators really want to accomplish something, they would be well advised to decertify security-anemic 911 systems. Virginia did that for the WINVote balloting system when they were faulted for inappropriate precautions in "physical controls, network access, operating system controls, data protection, and the vote tally process" (http://elections.virginia.

gov/WebDocs/VotingEquipReport/WINVote-final.pdf). The government might be able to copy and paste directly from the Virginia report since the problems aren't dissimilar.

LEGISLATIVE BRIGHT SPOTS

The legislative news isn't all deplorable. This year some states are considering legislation to address interception of cell phone communication, such as IMSI catching, that's been widely adopted by law enforcement and private security interests. In April, Washington state similarly proposed reasonable extensions to statutes on communication interception and pen registers that require warrants for the use of IMSI catchers (http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/House%20Passed%20Legislature/1440-S.PL.pdf). Other states like California approach the problem from a procedural point of view, seeking to ensure that the appropriate safeguards are in place to protect the data (https://legiscan.com/CA/text/SB741/2015). In the long term, my hunch is that the Washington state model will predominate, although it could take a few constitutional court challenges before that happens. All in all, this sort of legislation is headed in the right direction: it puts the onus on institutional abusers to clean up their act and veers away from adding to our increasing prison populations.

Another strong piece of legislation deals with mobile-related location privacy. Civil libertarians will appreciate that some states are requiring government officials and law enforcement to get warrants before accessing mobile device GPS coordinates. Once again the states are leading the way with Maine, Montana, New Hampshire, and Utah having recently passed robust laws in defense of personal privacy, whereas weaker laws were passed in Colorado, Tennessee, and Virginia. The most interesting points of difference involve the level of privacy protection and exceptions to the warrant requirements (for example, user consent, emergency circumstances, whether the device has been reported stolen, and so on). The Center for Democracy and Technology published an informative survey online on 23 July 2015 that compares these state efforts with links to the specific statutes.[24]

In an attempt to unify state efforts, Senator Ron Wyden (D-OR) and Congressman Jason Chaffetz (R-UT) introduced the same legislation to the Senate (S237; www.congress.gov/bill/114th-congress/senate-bill/237/text) and House of Representatives (HR491; www.congress.gov/bill/114th-congress/house-bill/491/text) on 22 January 2015. The congressional bills are more expansive, provide some penalties, and allow considerable exceptions for investigative and surveillance agencies. Overall, the states are quickly rising to the occasion with more reasonable proposals.

Will kill switches be mandated? Will the FBI get its tiny screen doors? Will we continue to incarcerate people for exploiting a 911 dispatch system that is an attractive nuisance to script kiddies and miscreants? Stay tuned.

REFERENCES

1. M. Schwartz, "The Trouble with Smartphone Kill Switches," *Information Week*, 13 Aug. 2013; www.informationweek.com/mobile/the-trouble-with-smartphone-kill-switches/d/d-id/1111143.
2. M. Schwartz, "Smartphone Theft: What Is Best Defense?," *Information Week*, 16 May 2013, www.informationweek.com/mobile/smartphone-theft-what-is-best-defense/d/d-id/1109986.
3. M. Williams, "California Bill Proposes Mandatory Kill-Switch on Phones and Tablets," *PCWorld*, 7 Feb. 2014; www.pcworld.com/article/2095640/california-bill-proposes-mandatory-killswitch-on-phones-and-tablets.html.
4. M. Lifsher, "Bill That Would Require Smartphone Kill Switches Is Close to Passage," *The Los Angeles Times*, 3 Aug. 2014; www.latimes.com/business/la-fi-capitol-business-beat-20140804-story.html.
5. Smartphone Crime Prevention Act, Bill, 113th United States Congress, 2nd Session, 2014; www.washingtonpost.com/blogs/the-switch/files/2014/02/KillSwitchBill.pdf.
6. M. Williams, "US Carriers Said to Have Rejected 'Kill Switch' Technology Last Year," *PCWorld*, 24 Feb. 2014; www.pcworld.com/article/2100940/us-carriers-said-to-have-rejected-kill-switch-technology-last-year.html.
7. R. Faturechi, "Google, Microsoft Agree to Compromise on 'Kill Switches,'" *The Los Angeles Times*, 19 June 2014; www.latimes.com/business/technology/la-fi-tn-google-microsoft-kill-switches-20140619-story.html?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheTechnologyBlog+%28Los+Angeles+Times+Technology+Blog%29.
8. M. Lafsher, "Bill that Would Require Smartphone Kill Switches Is Close to Passage," *The Los Angeles Times*, 4 Aug. 2014; www.latimes.com/business/la-fi-capitol-business-beat-20140804-story.html.
9. "Mobile Phone Insurance Market Shares," *Warranty Week*, 14 Nov. 2013; www.warrantyweek.com/archive/ww20131114.html.
10. J. Bamford, *The Puzzle Palace*, Penguin Books, 1983.
11. V. Sussman, *Lost in Kafka Territory: The Feds Go after a Man Who Hoped to Protect Privacy Rights*, Electronic Frontier Foundation, 3 Apr. 1995; https://w2.eff.org/legal/cases/PGP_Zimmermann/sussman.article.
12. J. Warren, "The Persecution of Phil Zimmerman, American," blog, 4 Apr. 1995; http://contra.org/pgp/PhilZimmerman.html.
13. J. McLaughlin, "FBI Director Says Scientists Are Wrong, Pitches

Imaginary Solution to Encryption Dilemma," *The Intercept*, 8 July 2015; https://firstlook.org/theintercept/2015/07/08/fbi-director-comey-proposes-imaginary-solution-encryption.
14. "Some Kind of Frontdoor Key," video, CSPAN, 10 July 2014; http://www.c-span.org/video/?c4543920/kind-frontdoor-key.
15. J.B. Comey, speech to the Brookings Institution, 16 Oct. 2014; www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
16. B. Gage, "What an Uncensored Letter to M.L.K. Reveals," *The New York Times*, 16 Nov. 2014; www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html?_r=0).
17. T. Timm, "We're Suing the Justice Department over FBI's Secret Rules for Using National Security Letters on Journalists," *BoingBoing*, 31 July 2015; http://boingboing.net/2015/07/31/were-suing-the-justice-depar.html.
18. M. McConnell, M. Chertoff, and W. Lynn, "Why the Fear over Ubiquitous Data Encryption Is Overblown," *The Washington Post*, 28 July 2015; https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.
19. N. O'Connor, "Encryption Makes Us All Safer," Center for Democracy & Techology, 8 Oct. 2014; https://cdt.org/blog/encryption-makes-us-all-safer.
20. D. Froomkin and N. Vargas-Cooper, "The FBI Director's Evidence against Encryption Is Pathetic," *The Intercept*, 17 Oct. 2014; https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb.
21. J. McLaughlin, "FBI and Comey Find New Bogeyman for Anti-Encryption Arguments: ISIS," *The Intercept*, 7 Jul. 2015; https://firstlook.org/theintercept/2015/07/07/fbi-finds-new-bogeyman-anti-encryption-arguments-isis).
22. H. Abelson et al., "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *DSpace@MIT*, 6 Jul. 2015; http://dspace.mit.edu/handle/1721.1/97690.
23. C. Dameff, P. Hefley, and J. Tullly, "Hacking 911," video, DEF CON 22, Aug. 2014; www.youtube.com/watch?v=mBOLml3yLBY.
24. "Survey of State Location Privacy Legislation," Center for Democracy & Technology, 23 July 2015; https://cdt.org/insight/survey-of-state-location-privacy-legislation.

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.

Selected CS articles and columns are also available for free at **http://ComputingNow.computer.org**.