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 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.

---

**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.
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. 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 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 (which is referred to by its original acronym, 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. However, they have no problem with legislation that penalizes users who reprogram phones—whether stolen or not.

Manufacturer and vendor incentives converge around protecting unimpeached 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 of the other large 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.

**Incentives for passage**
Some stakeholder communities support kill-switch legislation. For one, the typical mobile device owners 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 a public good. This naive view is shared by the majority of politicians.

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. The only chance of preventing this kind of infiltration would be to deploy robust
encryption with open source software

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

egory, 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 wireless service revenue. 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.

What’s Next?
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 struggle with 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 the 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 prepublication censorship for all scholarly papers involving cryptography.6 A committee of representatives from the professional societies (including ACM, the Computer Society, and IEEE) that published 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.

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.7 The persecution was apparently even extended to those who wrote op-ed pieces about Zimmerman’s plight in Bay Area newspapers.8 Nothing so offends authoritarianists 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.9 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 couldn’t 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.10

Comey’s presentation to the Brookings Institution on 16 October 2014 provides a clearer statement of his opinion.11 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 about COINTELPRO showed, the FBI has a decades-long history of highly questionable surveillance, wiretaps, and sundry black-bag operations against US citizens—including sending suicide notes to Martin Luther King Jr.12 Recently, it’s become fashionable for the FBI to use National Security Letters (NSLs) and “exigent letters” to spy on citizens and journalists,13 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, former high-ranking national security and defense officials 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: “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.” Encryption makes us safer.

The Intercept goes further in debunking the FBI’s claims that encryption interferes with effective prosecution of criminals. 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 kinds 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.

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.

But by far the most important argument against government backdoors, 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 Communicating 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 ambition 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 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 dif-

---

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.
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. The same can be said of location-spoofing apps for mobile devices—the provider might be 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 intimidation, 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.

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/hr_2031/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.”

Without question, the primary cause of swatting and other 911 vulnerabilities is an immature approach to information 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 US 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://lawfilesexit.leg.wa.gov/biennium/2015-16/Pdf/Bills/House%20Passed%20Legislature/I440-S.P.L.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. 23

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
12. J. McLaughlin, “FBI Director Says Scientists Are Wrong, Pitches Imaginary Solution to Encryption Dilemma,” The Intercept, 8 July 2015;


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.