Cutter
IT Journal

The Journal of
Information Technology Management

Vol. 28, No. 7
July 2015

Mitigating the Risks of Technology Backlash

"Technological advances have without doubt improved societal wealth, health, and standards of living. However, for all the tangible benefits technology creates, there is a growing disquiet that perhaps the risks of technology are beginning to outweigh its rewards."

— Robert N. Charette, Guest Editor

CUTTER CONSORTIUM

Technology Abuse and the Velocity of Innovation

by Hal Berghel

TECHNOLOGY ABSURDISM

Technology absurdism is the development of technology that ignores, fails to appreciate, or underrepresents obvious negative externalities.[1] Let me show you what I mean with a few examples.

Rust? Never Heard of It

In the past year, the US National Highway Traffic Safety Administration announced the recall of defective Takata air bag inflators in nearly 34 million automobiles,[2] the largest recall in US automotive history. After several years of study, Takata has reached a "preliminary conclusion" as of 18 May 2015 that the inflators can rupture. No news there — the victims had that figured out on impact. Takata reports that "it appears that the inflator ruptures have a multi-factor root cause that includes the slow-acting effects of persistent and long-term exposure to climates with high temperatures and high absolute humidity"[3] (read: they rust and don't stand up to heat). Takata has determined empirically in their lab that .51% of the inflators in hot and humid climates will rupture. They estimate that .25% of passenger airbags deploy in the field each year. So if you're unlucky enough to own one of the recalled cars that were operated in hot and humid environments for a while, your risk of wearing metal shard cologne may approach one in a thousand this year.

That the Takata airbags were not ready for prime time is really not at issue here. Let's analyze this recall from the point of view of product development and engineering. The analytical substance is as simple as our father's admonition not to leave his tools outside when we're done with them. Rust is not a foreign concept that is just now creeping into our technical vocabulary. For the past few millennia, it has been associated with iron and moisture. Just what manner of metallurgy was Takata using that ignored the combined effects of moisture and heat on steel parts? The real story behind this recall has to do with accelerated prototyping and rush-to-market, inadequate product testing, lax oversight, a risk-benefit analysis gone awry, and a preoccupation with cost savings. All of these combined in a race to the bottom in terms of product safety involving technological shortcomings known since the Iron Age.

It Depends on What You Mean by "Prevent"

The proximate cause of the Takata recall is not too dissimilar from the 2010 Gulf of Mexico oil spill. On 20 April of that year, the BP Horizon exploration rig blew up. It was located 49 miles off the coast of Louisiana and drilling at a depth of more than three miles below sea level. Eleven crewmembers lost their lives, others were injured, and the largest oil spill in US history resulted. In January 2011, President Obama's National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling reported that this accident was entirely avoidable and due to failures at all levels of management.[4] But there are shades of Takata in this story as well.

A fail-safe device — a "blowout preventer" — was in place at the time of the spill. It was specifically designed to prevent what happened from happening, management failures or not. But this blowout preventer's "deadman" system failed to deploy during a poorly implemented temporary abandonment procedure. It seems that no one had bothered to test the blowout preventer to see if it would work in this application! As a consequence, lives were lost and 5 million barrels of crude polluted the Gulf of Mexico. The blowout preventer is the analog of the airbag inflator!

The Cost of Doing Business

There is another variation on technology absurdism that bears mention. This results when a technology solution for a known risk is both understood and available but is intentionally not used, usually for economic or political reasons. The delayed introduction of seat belts by the automobile industry was a product of the latter's risk-benefit analysis: it was more cost-effective to settle with the victims after an injury than to invest in seat belts to prevent the injury. A current example of this reasoning is to be found in recent resistance by the US rail

industry to introducing positive train control (PTC), which can automatically stop a train to prevent certain kinds of accidents from occurring. The Amtrak derailment in Philadelphia on 12 May 2015, which resulted in eight deaths and over 200 injuries, highlights the dangers inherent in letting cost override safety considerations. The value of PTC has been understood for decades, but weak congressional resolve allows the rail industry to avoid the expense.[5] As a data point, the 2008 Rail Safety Improvements Act,[6] which mandated that each Class I rail carrier develop a plan for PTC by 31 December 2015 and have it installed by 31 December 2018, is not likely to be enforced anytime soon. At the request of the rail industry, several US senators have proposed that even the 2018 date be deferred.

Congressional response to the ever-increasing risk, combined with the growing unprofitability of Amtrak, led to a 1994 law that capped the single accident limit at US $200 million (or $126 million in 2015 dollars).[7] This is classic political reasoning: reduce the risk to the political donor class by limiting the liabilities of potential claimants. History has recorded the effect. The disastrous train collision that took place in the Chatsworth district of Los Angeles in 2008 pushed casualty liabilities so far beyond this cap that the presiding judge had to lower the cash payout he calculated by 25% to fit within the legal limit.[8] From the point of view of politicians, and the transportation industry that supports them, lowering the settlement cap and delaying implementation of PTC is preferable to investing in public safety, as long as there are no criminal penalties that accrue to the transportation executives and the civil penalties remain modest. It's just the cost of doing business, much the same way that moral hazards are handled in banking and finance.[9]

Technology absurdism is an epidemic that needs to be addressed. The solution is neither obvious nor easy to implement, and those of us in positions of technology leadership, or who are domain knowledge experts, need to take responsibility for a measurable part of problem.

DIGITAL WRIGHTS MANAGEMENT AND ENERVATION

The realm in which technology absurdism reigns supreme is information technology. Low entry-level costs, easy access to computers and networks, widespread availability of high-quality malware, a wide base of development software, and huge potential markets for inexpensive products make this the absurdist's environment of choice for poorly thought through ideas.

Pillow Talk

My favorite exemplar at the moment is my new WiFi-enabled bed.[10] I know what you're saying: sure this bed will work with Static IP, but can it work within a Class C sleep space served through DHCP? Well, yes it can. And, of course, both Apple iOS and Android apps are available for your smartphone.

Now I understand the allure of functional product differentiation, but I'm not seeing the unique sales proposition here. Rather, this slumber feature tells me that there are too many STEM graduates who have too much time on their hands. In this case, we'll refer to the anonymous enervators collectively as "bedwrights" and subsume the fruits of their labors under the newest form of intellectual property protection: digital wrights management (DWM). Similarly, those who might seek to circumvent DWM shall be known as hacklers, as in "She's being prosecuted for hackling into the CEO's Web bed." What is the appropriate boudoir information security policy? Would porting over the default policy from the family room be considered an egregious breach of our trust model? Inquiring minds want answers.

The realm in which technology absurdism reigns supreme is information technology.

Could've Seen That Coming

Surely one of the most egregious breaches of digital best practices as well as truth in advertising was the recent TRENDnet IP Security Camera public relations fiasco.[11] According to the US Federal Trade Commission (FTC) complaint,[12] TRENDnet's SecurView IP cameras were never all that "secur." Specifically, it alleges that the "respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras," including transmission and storage of login credentials in cleartext, failure to respond to user and third-party vulnerability reports, and failure to test their bundled software. By the time of the FTC complaint, hackers had posted links to 700 Internet-connected security cameras for all to see. After two years and extensive media coverage, TRENDnet patched their software. On 16 January 2014, the FTC ordered TRENDnet to introduce security protection into their SecurView product line that is consistent with their product representations.[13]

My objective here is not to beat up on TRENDnet — for they have wandered no further afield of citizens' privacy expectations than other high-tech companies[14] — but to reinforce the point that technology absurdism in one form or another is rampant. In this case, TRENDnet failed to embrace any reasonable interpretation of industry best practices for Web video security and privacy since the earliest days of the Web. In terms of user security and privacy, the operational differences between the SecurView Web camera system and the analog baby monitors of the 1990s were purely cosmetic.

There are several categories of technology that positively invite technology absurdism.

A Banner Decade (for Hackers)

It is worth mentioning in this regard that some of us feel that the concept of the Internet-enabled security camera is still not ready for prime time. One of the attack vectors exposed in the TRENDnet and related compromises is actually a TCP/IP feature, namely that IP-addressable services require service banners in order to function. So-called Internet banners are really only the protocol headers offered by the servers for session negotiation (protocol version supported, server-side Web software and version numbers, etc.). This information must be public because it is required for the connection to work. But these banners all too frequently give up more information than needed, such as default passwords, GPS data, and configuration settings. This applies to all common TCP/IP protocols, including those used by industrial controllers, traffic signals, nuclear power plants, and other miscellaneous componentry in our ill-conceived Internet of Things.

In fact, there is a search engine designed specifically to search for Internet banners: Shodan.[15] Shodan now searches for over 170 Internet banners in much the same way that Web search engines locate HTML data. What is more, Shodan was launched a year before TRENDnet's undersecured Web cameras were first sold. From any reasonable security and privacy perspective, exposing security camera imagery to the entire Internet has never been a good idea, and connecting a camera (or baby monitor, or what have you) to any network without verifiably robust security practices in place has been downright irresponsible for most of the past 50 years.

Be that as it may, the FTC's complaint against TRENDnet was twofold: best security practices weren't followed, and, more importantly, the corporate claims of security and privacy protections were vast overstatements if not downright misrepresentations.

As I write this, Omron, a manufacturer of programmable logic controllers, makes the following claim of their product:

> ... the security risk [of using Omron PLCs] is very low. Hackers and other evildoers, when they are attempting to "hack" into a network, usually go through a process of Port Snooping to determine what UDP and TCP ports on a router are open and connected to a PC (vulnerable). Standard Ethernet communication protocols are used in this process. When a router is forwarding a TCP or UDP port to an Omron PLC, the traffic is being delivered to a non Windows based operating system. *This makes the PLC impenetrable to standard hacking methods*."[16] (italics added)

The quoted analysis goes well beyond naïve and uninformed. It amounts to digital blasphemy. That this report remains online and was reported on the Shodan blog on 9 February 2015 should not be overlooked!

TECHNOLOGIES THAT ARE RIPE FOR ABUSE

What's the Frequency, Kenneth?

Let's move from the specific to the general. There are several categories of technology that positively invite technology absurdism. Certainly the use of radio frequency (RF) technology — whenever privacy and security are of concern — is at the vanguard of this movement.[17] Examples of engendered RF mistakes include the Western Hemisphere Travel Initiative's passive RF-based PASS card, which showcases the military-industrial-surveillance complex's penchant for technology absurdity. Another is the deployment of RFID cards and tags modeled on faith-based security standards (read: if I wish it to be secure, then, by definition, it is).[18] A third example is the development of the Wired Equivalent Privacy protocol in 802.11 WiFi.[19] This last example has the additional twist that the vulnerability was actually built into the IETF standard. As I've written about these topics elsewhere, I'll suppress the temptation to elaborate here.

Can't Fight the (Global Positioning) System

Another technology that is just ripe with opportunity for technology abuse is the Global Positioning System (GPS). GPS distinguishes itself by offering both a security *and* a privacy vulnerability. From the security

perspective, commercial GPS is easily spoofed.[20, 21] This is easily understood if one thinks back to the Clinton Administration's elimination of Selective Availability (SA) in May 2000. One may recall that in years prior, accuracy was measured in tens of meters. After SA was eliminated from commercial GPS, accuracy increased to within a few meters on average. Spoofing in this sense is just a way of turning SA back on through "satellite cloning." It arises because commercial GPS uses triangulation based on unencrypted and unauthenticated signals. As with RF systems generally, connection is established with the strongest available signal. So any GPS signal that "spoofs" a legitimate GPS satellite signal with a stronger one can provide data that will be used by the triangulation algorithms. Todd Humphreys, director of the University of Texas at Austin's Radionavigation Laboratory, has demonstrated empirically that spoofing can easily produce GPS "blunders" (triangulation error measured in miles).[22]

Not only was GPS spoofing understandable at the design stage, its use as a vulnerability was entirely predictable. (For this reason, the US military adopted an anti-spoofing module over a decade ago.) However, that doesn't help the typical commercial GPS user. This is to say nothing about the triviality of GPS jamming where a criminal or terrorist wants to produce a crash but isn't terribly invested as to time and place.

Mind My Dots, Maparella

Perhaps more insidious is the use of GPS dots[23] — micro GPS transponders about the size of a slice of a typical pencil eraser that may be used to triangulate to a position. Absent regulation, GPS dots will become inexpensive and ubiquitous in the years to come. That will result in GPS dots becoming the surveillance target of choice by snoops everywhere — government spy agencies, divorce attorneys, law enforcement, government contractors, criminals, and predators alike. Only in this case, abuse of such trackers will not run afoul of government regulators, at least not in the US. To my knowledge, there is no federal statute that regulates such surveillance by nongovernment interests.

THE DEVOLUTION OF INNOVATION

I offer for your consideration "Gresham's Twist on Moore's Law" — namely, that the world's capacity to create absurd technology doubles every 18 months, where absurd technology is to be understood in the sense explained above. Technology absurdism is unique to our postindustrial Information Age, in which the velocity of innovation has increased to the point that it is often unbridled by adequate reflection, complete context, understanding, and oversight. This was not the case in the kinetic and analog world of our parents and grandparents. While they may have lived in a Rube Goldberg world, we live in a world defined by hazards identified by George Orwell and Aldous Huxley.

It is precisely this velocity that is the cause for concern. Innovation came gradually to the Industrial Age. Morse's wired telegraph (1837) was separated in time from Marconi's wireless telegraph (1894) by over a half-century. That provided an ample temporal palette for refinement and contextualization. It also enabled society time to adapt. Note that Wheatstone's ABC character input telegraph (1840), Bain's facsimile machine (1843), Hughes's keyboard telegraph (1855), Bain's chemical paper printer (1846), Phelps's motorized teleprinter (1880), and the message-routing telex system (1930) were spread out over nearly a century after the invention of the telegraph. That allowed each innovation to mature at more or less its own speed, building upon past achievements, finding its own niche, and, for the most part, negotiating a responsible pathway to market. Had all of these advances occurred in the same decade, technological chaos would have worked against their maturation process.

While our parents and grandparents may have lived in a Rube Goldberg world, we live in a world defined by hazards identified by George Orwell and Aldous Huxley.

In effect, that's the problem high-tech innovation faces today. I like to think of this as technology devolution (in the biological sense), where there isn't time for the technology equivalent of natural adaptation to take effect. Progress is blocked because mutations take place more or less randomly, concurrently, and independently. Had this happened in biology, Darwin would have documented wildly implausible and ephemeral organisms that devolved into chaos rather than evolved into order. Biological devolution would lead from complex life forms to those more primitive and purposeless. However, the devolution of high-tech innovation turns otherwise useful technology platforms into those of dubious value that may work against society's interests. Not that this effect is intended. It is produced by errors of omission rather than commission. Society lacks the

time to detect and purge the worst of the bad ideas before widespread adoption. This responsibility is left to technologists.

Unfortunately, in this devolutionary climate, we have the worst ahead of us. Poorly designed vehicle telematics are easily hacked, turning microlevel controls used by antilock braking systems into nightmarish hazards at freeway speed. RF-enabled pacemakers and insulin pumps invite hacking. Cell phone kill switches (now required in many jurisdictions) offer a bouquet of incentives for the criminal elements, from bricking mobile devices as a barrier to evidence collection to preventing victims from calling for help. Microtaggants abound for misplaced surveillance and invasion of privacy. Perfluorocarbon scent emitters are ideal for covert tracking of the unwary. Add to that an expansion of drone space without antecedent community agreement on privacy expectations, driverless cars and robots that invite weaponization, and the ill-conceived Oregon mileage-based gas tax (which, by taxing miles driven rather than gas consumed, actually penalizes fuel efficiency), and our future looks dim even by the standards of Orwell and Huxley.

The velocity of technology innovation needs to be throttled to the point where society can control it.

With innovation occurring at current velocities, wherefrom are the best practices to spring? The answer is not to be found in industry, for companies are incentivized to accelerate the introduction of new products rather than reflect on how well they serve society. Nor is the answer to be found in a political process fueled by special interests. Higher education can certainly play a role, but only if there are courses that deal with regulating innovation as a social good, rather than racing toward it for economic reasons. If there are such courses, I haven't seen them, and they're unlikely to fit well into the entrepreneurship programs so much in vogue these days. I'm not at all confident that academic leadership will rise to this challenge anytime soon.[24]

That pretty much leaves technology leaders, who must include some understanding of how to identify the potential negative externalities of an innovation before deploying it. In each of the examples I gave above, competent domain experts knew, or should have been able to anticipate, the potential abuses that resulted. This is indeed not "rocket science." That's not to say that technology leaders can deflect an organization's first-to-market mentality, but they can inform and document potential negative externalities in white papers for corporate and government leaders to consider. Our industry demands more iconoclasts!

If we accept the premise that not everything we can do is worth doing (not an unreasonable assumption), the preposterousness of accelerating innovation without full consideration of negative consequences is easier to spot as an absurdity. The velocity of technology innovation needs to be throttled to the point where society can control it. And there are no external controls that are adequate to this challenge. Knowledge domain experts are the appropriate change agents lest the executives remain stuck on stupid. This is not Luddism, but lucidity.

ENDNOTES

[1]Berghel, Hal. "Noirware." *IEEE Computer*, Vol. 48, No. 3, March 2015.

[2]"Takata Air Bag Recalls." Safercar.gov, 2015 (www.safercar.gov/rs/takata/takatalist.html).

[3]"Defect Information Report 15E-043-2." TK Holdings Inc., 18 May 2015.

[4]"Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President." National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, January 2011.

[5]Flegenheimer, Matt, et al. "Amtrak Crash Illuminates Obstacles to Plan for Controlling Train Speeds." *The New York Times*, 18 May 2015.

[6]*Federal Rail Safety Improvements*. Public Law 110-432, 16 October 2008.

[7]"Limitations on Rail Passenger Transportation Liability." US Code, Title 49, Section 28103, 2 December 1997.

[8]Williams, Carol J. "Compensation Determined for Metrolink Crash Victims." *Los Angeles Times*, 15 July 2011.

[9]Berghel, Hal. "The Future of Digital Money Laundering." *IEEE Computer*, Vol. 47, No. 8, August 2014.

[10]"Tempur-Ergo Grand Complete Reference Guide." Tempur-Pedic Management, LLC, 2013 (www.tempurpedic.com/assets/pdfs/TEM-TEMPUR_Ergo_Grand_Owners_Manual_MAR_15.pdf).

[11]Hill, Kashmir. "Camera Company That Let Hackers Spy on Naked Customers Ordered by FTC to Get Its Security Act Together." *Forbes*, 4 September 2013.

[12]"In the Matter of TRENDNET, Docket C-4426: Complaint." US Federal Trade Commission (FTC), 16 January 2014 (www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf).

[13]"In the Matter of TRENDNET, Docket C-4426: Decision and Order." FTC, 16 January 2014 (www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf).

[14]Maass, Peter. "Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless." *Wired*, 28 June 2012.

[15]Shodan (www.shodanhq.com).

[16]Hughes, Jay. "How Safe Is Allowing Remote Access to Omron PLCs Via the Internet and How Is It Accomplished?" Omron Electronics, LLC, 2009 (https://goo.gl/A66RTY).

[17]Berghel, Hal. "RFIDiocy: It's Déjà Vu All Over Again." *IEEE Computer*, Vol. 46, No. 1, January 2013.

[18]Berghel (see 1).

[19]Sthultz, Michael, Jacob Uecker, and Hal Berghel. "Wireless Insecurities." In *Advances in Computers*, Vol. 67, edited by Marv Zelkowitz. Elsevier, 2006.

[20]Berghel (see 1).

[21]Humphreys, Todd. "The GPS Dot and Its Disconents: Privacy vs. GNSS Integrity." *Inside GNSS*, March/April 2012.

[22]Humphreys (see 21).

[23]Humphreys (see 21).

[24]Berghel, Hal. "Borderline Executive Disorder." *IEEE Computer*, Vol. 48, No. 4, April 2015.

Hal Berghel is currently Professor of Computer Science at the University of Nevada, Las Vegas, where he has previously served as Director of both the Schools of Computer Science and Informatics, and as Associate Dean of the College of Engineering. In 2005, Dr. Berghel created and directed Nevada's first CyberSecurity degree programs (bachelor's, master's, and PhD), which became an NSA Center for Academic Excellence. He was the founding Director of the Identity Theft and Financial Fraud Research and Operations Center and CyberSecurity Research Center. His research interests are wide-ranging within the binary and digital ecosystem, ranging from logic programming and expert systems to relational database design, algorithms for non-resolution-based inferencing, approximate string matching, digital watermarking and steganography, and digital security and privacy. Since the mid-1990s, Dr. Berghel has applied his work in digital security to law enforcement and intelligence gathering, particularly with respect to digital crime, digital money laundering, information warfare, and trusted identities. His research has been supported by both industry and government for over 30 years. In addition to his academic positions, Dr. Berghel is also a popular columnist, author, frequent talk show guest, inventor, and keynote speaker. For nearly 15 years he wrote the popular "Digital Village" column for the Communications of the ACM*, and he has written the "Out-of-Band" column for* IEEE Computer *since 2011.*

Dr. Berghel is a Fellow of both the IEEE and the ACM and serves both societies as a Distinguished Visitor and Distinguished Lecturer, respectively. He has received the ACM Outstanding Lecturer of the Year Award four times and was recognized for Lifetime Achievement in 2004. He has also received both the ACM Outstanding Contribution and Distinguished Service awards. Dr. Berghel is also the founder and owner of Berghel.Net, a consultancy serving government, business, and industry. He is a member of the Nevada Technology Crimes Advisory Board and chairs the Nevada Privacy Subcommittee. He can be reached at hlb@berghel.net.

Cutter IT Journal

The Journal of Information Technology Management

Begin a new, one-year subscription to Cutter IT Journal and Save 50%!

Your Front-Row Seat to IT Management Debate at the Highest Level!

Every day, your organization is confronted with the stark reality of having to achieve more aggressive goals with a shrinking budget, ever-changing requirements, and impossible deadlines.

Few of you have the time to develop well-supported arguments on how to get your organization to improve its operations. It's a tough trap; you know solutions are out there, but you're too busy to identify them and convince your organization to implement them.

Monthly Advice, Solutions, and Experience You Can Rely On

A ***Cutter IT Journal*** subscription helps you break out of the trap. Every month, ***Cutter IT Journal*** features a select guest editor who articulates the controversial issues, offers his or her opinion on them, invites others to introduce opposing viewpoints, and sparks a lively debate.

With five to seven articles in each issue, ***Cutter IT Journal*** provides you the opportunity to experience a variety of perspectives on a topic and serves as an international forum for debate of technology issues. The thoughtful discourse delivered in ***Cutter IT Journal*** will help you solve the challenges you are facing in your organization today.

Cutting Edge Topics

Cutter IT Journal addresses important business and technology issues such as security and risk management, digital technologies, data analytics, enterprise architecture, agile management, emerging technology trends, innovation, sourcing, digital transformation, business technology strategies, and more.

Weekly Email Advisor

You'll also receive the weekly emailed ***Cutter IT Advisor,*** bringing you practical advice and thoughtful analysis from well-known and respected experts in the field.

Digital and Print Delivery

As a subscriber, you'll receive your monthly copy in the mail as well as both an e-pub and pdf version by email.

SPECIAL OFFER

Begin your subscription to ***Cutter IT Journal*** today and **save 50%** off the regular subscription rate! Plus receive all 2014 issues **FREE** on a flash drive!

To subscribe for just $242 ($342 outside N. America) and receive your FREE flash drive, go to **bit.ly/CITJ50**. Or complete and return the form below by fax to +1 781 648 8707, call +1 781 648 8700, or email sales@cutter.com.

For more information on ***Cutter IT Journal***, please visit www.cutter.com/itjournal.html.

Visit the Cutter Bookstore!

Visit **bookstore.cutter.com** to order individual ***Cutter IT Journal*** issues and to see more of Cutter's technology resources.

Special Offer: Save 50% on a New Subscription Today!

CUTTER CONSORTIUM

☐ ***YES!*** Please start my new, one-year subscription to ***Cutter IT Journal*** for just $242 (US $342 outside N. America) — I save 50% off the regular rate of $485/US $585! Plus send all 2014 issues on a flash drive!

Name	Title
Company	Dept.
Address/PO Box	Mailstop/Suite
City	State/Province
ZIP/Postal Code	Country
Phone	
Fax	
Email	

Fax to +1 781 648 8707, call +1 781 648 8700, or send e-mail to service@cutter.com. Mail to Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA. Order online at bookstore.cutter.com.