

UBIQUITY REQUIRES REDUNDANCY



The Case for Federal Investment in Broadband

By Mark Lloyd

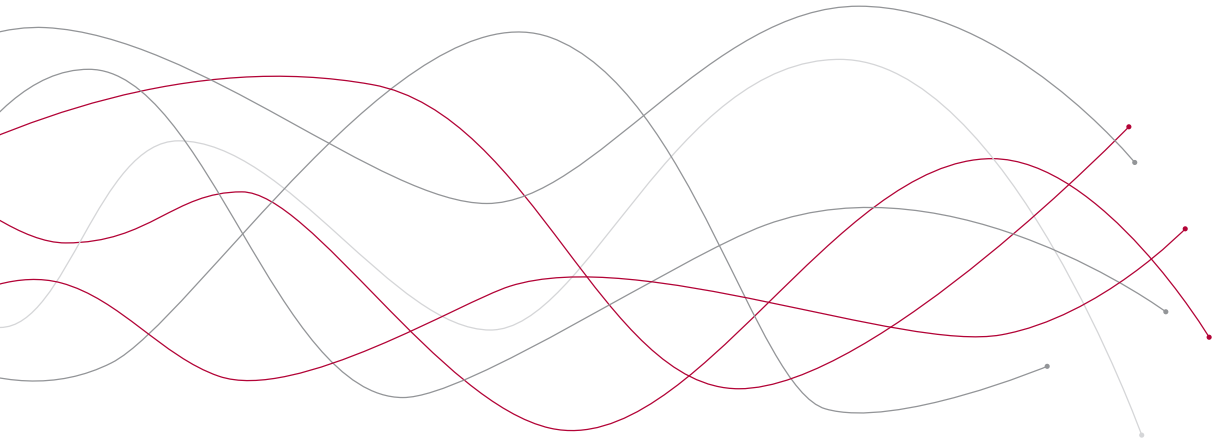
THE UNITED STATES WILL NOT MEET President Bush's goal of universal broadband by the end of 2008—not by a long shot. The number of subscribers to Internet services is growing faster than the adoption of “dial-up,” yet for the most part these subscribers are not connected to the broadband technology Congress described in 1996 as a two-way communications service capable of high-speed delivery of data, voice, and video.

This failure to connect over half the country to advanced telecommunications service is not a technological failure. It is a 21st century public policy failure. In the 1990s, policies established by the Clinton administration to encourage public/private telecommunications partnerships, to connect schools and libraries to the World Wide Web, and to allow competitive service providers onto the networks of the local telephone monopolies all sped up

the deployment of broadband around most of the nation. These policies were either deliberately abandoned or hampered by the Bush administration.

The increasing noise from Washington about the lack of a U.S. broadband policy obscures the fact that a policy choice was made by the Bush administration to rely entirely on “market forces” to determine how and where advanced telecommunications services would be deployed. That policy has failed.

The goal of federal investment in broadband should be first and foremost to ensure our ability to respond to threats to our homeland security and to natural disasters. And the result of administration neglect, industry intransigence, and the incompetence of a Federal Communications Commission apparently “captured” by the industry it is supposed to regulate has left the American people and most



policymakers with no clear idea where broadband services are deployed in the United States.

There is no credible dispute that the United States has fallen behind Canada and France and Japan and a dozen other industrial countries in broadband deployment.² Americans are not more adverse to new technology compared to our neighbors to the north or our friends overseas. The difference is that these countries have moved ahead of the United States after having adopted one version or another of U.S. telecommunications policies established in the mid-1990s.³

In addition to leaving America less competitive in a global economy, this failure has left the nation vulnerable and ill-prepared for real threats to our national security—the rationale behind the initial U.S. government investment in the development of the Internet.

The American invention of the Internet, of course, was preceded by hefty scientific investments beginning with the Eisenhower administration for military purposes. In fact, the Internet developed despite “market forces” dominated by the not-so-invisible hand of the Bell telephone monopoly. While the development of the Internet has certainly benefited from global market forces, the “free market” blinders that prevent present-day

U.S. policymakers from seeing beyond the interests of corporations must be removed. While Reagan-era Republicans seem to don their blinders with greater pride, this is not a partisan issue. It was, after all, Vice President Al Gore who insisted that the “information superhighway” would not be built the way the U.S. highway system was built, but would instead be financed by private enterprise.⁴

If the United States is to catch up with other developed and developing nations, however, we must look beyond even the abandoned policies of the Clinton era and begin to move with greater urgency and resolve to address pressing disaster response and defense needs. After all, the attacks of 9/11 and body blow of Hurricane Katrina highlight for all but the most doctrinaire advocates of free markets that there is an exceedingly strong case for direct government investment in the deployment of advanced telecommunications services to build a safe, strong, and resilient America.

The goal of federal investment in broadband should be first and foremost to ensure our ability to respond to threats to our homeland security and to natural disasters. Directly connected to this goal is the availability of advanced telecommunications services in our health care and educational systems—

the modernization of which is key to our nation's ability to respond to threats to our national security and public safety immediately and over the coming decades. Without ubiquitous broadband our first responders could be crippled by the lack of effective communications in the event of a terrorist attack or natural disaster. Similarly, our educational institutions need to be able to communicate quickly and effectively in case of a pandemic, as well as conduct R&D on all of the technologies needed to maintain our nation's national defense and public safety.

In meeting these goals, federal investment should make certain that the U.S. communications infrastructure is continually upgraded, robust, redundant, and able to withstand multiple threats and uses. The public should not be left to rely on any one technology, but rather on multiple technologies—each able to operate with the other, and each able to serve important needs if the other technologies are destroyed or compromised. Market forces will not guarantee this result.

INFRASTRUCTURE FOR A STRONG AND SAFE AMERICA

In small rural towns, in the crowded barrios and ghettos of urban U.S. cities, in those places where financial institutions are not yet convinced they can get an adequate return on investment, Americans do not have access to the communications networks they will need to keep them safe in the future.⁵ It is no coincidence that these same places hold our nation's toxic waste dumps, our chemical plants, and our seaports and airports, yet we do not have the ability to communicate most effectively where we are most vulnerable.

The Department of Defense has long been provided almost all the communication resources it needed to protect American interests overseas. What has been too often forgotten is the importance of equipping all Americans with the ability to participate effectively in the national defense effort at home. Americans take pride in assisting when

their communities are under attack or threatened by a natural disaster. A concerted effort must be made to equip all Americans so they are able to communicate effectively when confronted by catastrophe.

President Eisenhower understood the value of a robust transportation system at home to sustain national unity and to promote defense needs. In announcing the new interstate highway system, Eisenhower called the effort “the National Defense Highway System,” citing his direct experience with a problem-laden military convoy from Washington, D.C. to San Francisco he took in 1919.

Despite the squabbles of some local government and business leaders who fought against a federal highway system, Eisenhower was convinced that America could do better. As Richard Weingoff reports in his excellent history of the interstate system, when Vice President Richard M. Nixon delivered an address before a 1954 conference of state governors at Lake George, NY, reading from Eisenhower's detailed notes, he declared that the U.S. “highway network is inadequate locally, and obsolete as a national system.”

Nixon then recounted Eisenhower's convoy and then cited five “penalties” of the nation's obsolete highway network: the annual death and injury toll, the waste of billions of dollars in detours and traffic jams, the clogging of the nation's courts with highway-related suits, the inefficiency in the transportation of goods, and “the appalling inadequacies to meet the demands of catastrophe or defense, should an atomic war come.”⁶

If America is to be ready “to meet the demands of catastrophe or defense,” all Americans need access to advanced telecommunications services in the 21st century, just as they needed access to an advanced highway system in the 20th century. But as the 9/11 Commission noted in its report, the United States is not ready for a national emergency. And as every comprehensive analysis of the tragedy of Hurricane Katrina revealed, we are not prepared to handle a major natural disaster. Both of these experiences highlight the importance and the multiple failures

of U.S. communications services as warning systems or as systems to allow for the coordination of first responders.⁷

Command and Control vs. National Leadership

A standard complaint of conservative defenders of the current telecommunications regulatory system regarding communications policy focuses on the supposed “command and control regulatory policies” of the federal government.⁸ They argue that the heavy hand of regulation stymies the roll out of advanced telecommunications networks across the nation when in fact the tendency of the federal government historically is to exercise this “command and control” on behalf of the communications industry itself.

The result of this regulatory protection of different bits of the telecommunications industry leaves the United States with balkanized communications capabilities. If the prevention or response to the terrorist attacks on 9/11—when New York City police, fire, and rescue workers could not communicate with each other amid the chaos and carnage of that awful day—or the prevention or response to the failed levees overwhelmed by hurricane Katrina demonstrated anything, they demonstrated the need for better command and control.⁹

Indeed, in the debate over communications policy, the term “command and control” is little more than a right-wing slogan. Outside of military operations this phrase has never accurately described either the policymaking process or the execution of policy in the United States. Even the federal highway system so important to Presidents Roosevelt, Truman, and Eisenhower for military purposes, was the product of a contentious federal–state partnership.

Still, there is no question about the importance of federal vision and leadership and funding.¹⁰ The importance of strong federal engagement in the development of the national highway system is beyond dispute. The same can be said of the importance of federal leadership in the U.S. space program, which led to the U.S. satellite industry, as well as federal leadership

How our country's
critical communications
infrastructure is deployed
is entirely determined
by private industry.

in the Defense Advanced Research Projects Agency, which spurred the research behind the Internet.

Perhaps the most direct corollary to the national highway system in the U.S. telecommunications arena is the National Communications System. The NCS began after the Cuban missile crisis. Communications problems between and among the United States, the Soviet Union, and other nations helped to create the crisis. President Kennedy ordered an investigation of national security communications, and the National Security Council recommended forming a single unified communications system to connect and extend the communications network serving federal agencies, with a focus on interconnectivity and survivability.

The NCS oversees wireline (Government Emergency Telecommunications Service) and cellular service (Wireless Priority Service).¹¹ The NCS is now part of the Department of Homeland Security's Preparedness Directorate, and despite the increased attention to the communication needs of first responders on September 11, 2001, NCS failures and inadequacies were made obvious after Katrina.¹² In New Orleans, police officers were forced to use a single frequency on their patrol radios, which “posed some problems with people talking over each other,” explained Deputy Policy Chief Warren Riley at the time. “We probably have 20 agencies on one channel right now.” And with little power to recharge batteries, some of those radios were soon useless.

In southern Mississippi, the National Guard couldn't even count on radios. "We've got runners running from commander to commander," said Maj. Gen. Harold Cross of the Mississippi National Guard. "In other words, we're going to the sound of gunfire, as we used to say during the Revolutionary War."¹³ As Sen. John Kerry (D-MA) said: "This is a further demonstration of our inadequate response to the 9/11 Commission's recommendations and other warnings about the failures in our first responders' communications systems."¹⁴

How can these obvious communications failures still leave the United States groping for an adequate response? One of the biggest challenges we face is the tendency to see national defense and emergency needs regarding communications as separate and unrelated to the communications needs of the American public. The NCS has established an elaborate set of protocols that make government communications a priority over what is called the public switched network. Federal, state, and local governments pay substantial fees to use this communications network. But the determination over how that network is upgraded and deployed is entirely determined by private industry.

We cannot have a robust, survivable, interoperable communications system that protects the public if the public is treated merely as a mass of consumers and not as an integral part of national defense and emergency response. The U.S. public remains vulnerable because our communications infrastructure is too often viewed only as a private business. Katrina and 9/11 remind us that access to advanced telecommunications service is a public need. We need national leadership to remind us of this, and insist on policies that address public needs.

ADVANCED TELECOMMUNICATIONS CAPABILITY IN THE 21ST CENTURY

In the 1996 Telecommunications Act, Congress indicated that advanced information and communication technology, or ICT for short, should pro-

vide the ability to send and receive data, voice, and video. Today, advanced ICT means the ability to send and receive high-definition video in real time, something that requires massive telecommunications power if the goal is for everyone to be able to do so. Further complicating this goal is that in emergency situations communications systems become easily overloaded as people rush to their phones to check on loved ones.

In the case of an emergency or national disaster we need a capacity far greater than the market would support for even heavy shopping days. A starting point would be symmetrical speeds (both download and upload capability) of 10 gigabytes per second. Today, speeds of that magnitude are available only at the most important point-to-point interchanges of the Internet backbone or between dedicated military, financial, educational, or scientific institutions. Both fiber and robust wireless services have the potential to deliver these speeds in both directions.

But the construction of one or even two robust communications pipelines into police stations or military posts would still leave the United States vulnerable. The sole reliance on only one or two sources of communications creates an inviting target and, at the very least, creates the potential for deadly communications bottlenecks. Telecommunications businesses won't help us solve this problem. At their best, they work to create greater efficiency by eliminating redundancy. At their worst, they work to eliminate any and all competition so that even efficiency doesn't matter.

When reliability is essential, redundancy is highly valued. When lives are at stake, establishing alternative systems that can do as good a job as any designated primary system is routine. And while our policymakers speak of competition—sometimes even embracing competitive communications infrastructures that might lead to alternative "consumer" choice—policymakers rarely seem to understand that alternatives are essential to national defense and emergency preparedness.

Redundancy is so essential to public safety and national security that where private industry refuses to create these alternatives government must do so.

In fact, redundancy is so essential to public safety and national security that where private industry refuses to create these alternatives government must do so. Safety engineers consider redundancy a critical ingredient of creating a system with a high probability of safety. In the commercial aircraft industry, for example, pilots and passengers are assured of safety in part because redundant equipment, including engines and sensors, are required by government regulation.

In addition to redundancy, it is vital that the different systems and the equipment operating over these communications systems be interoperable. One unfortunate result of relying on private competition is the tendency of competitors to develop systems which do not permit interoperability. A key failing of emergency response after 9/11 and Katrina was the lack of interoperable communications equipment.¹⁵

Many of the problems of interoperability are the result of turf wars and not equipment limitations. Federal policies to override local turf wars are essential. The Department of Homeland Security has made it a priority to solve the range of problems related to interoperability.¹⁶ But again, interoperability must not be limited to operation over one infrastructure, but must cross all relevant communications platforms. Phones and computers

must operate over wireline and wireless infrastructure, including competing wireline and wireless networks. Interoperability is a vital component of emergency service and a modern communications network. Closed “private” broadband networks stifle not only innovation and service competition, they also limit the ability of all Americans to participate effectively in response to natural disaster and terrorist attack. If the United States is to compete effectively in a global economy and defend itself against global terrorist threats, then it must take advantage of the unique opportunities only possible with an open network.

Federal law should require that all broadband networks are open to the attachment of any equipment the user chooses—so long as it does not harm the technical operation of the broadband network. In addition, federal law should require broadband networks to be open to other information service providers and accessible to other networks, except for restrictions related to vital law enforcement or for network management.

Investing in Multiple Technologies

Our nation’s wireline infrastructure is inadequate to meet 21st century needs. The old telephone network is simply incapable of delivering the bandwidth to meet the emergency needs of today and the future. While efforts have been made to upgrade the relatively more modern cable infrastructure, there are too many rural communities where the cable system has not upgraded to provide digital service. Even in our major metropolitan areas, gross deficiencies are self-evident.

The strain on the existing telecommunications infrastructure was obvious as call after call was blocked during 9/11. But this strain is obvious to anyone who regularly uses either the Internet or regular cell phone service in a major metropolitan area in the United States. The concerns that the Internet as presently constructed simply will not bear the amount of use projected over the next

five years are longstanding. While more sophisticated filtering and better emergency protocols may address this problem in the short-term, the strain on the nation's telecommunications infrastructure will only increase as the call for greater bandwidth for video over the Internet increases.

If meeting the communications needs of first responders or panicked parents were simply a matter of "market forces," then one would be tempted to applaud the telephone and cable companies for squeezing as much profit as possible out of old technologies. But the challenge of communicating in an emergency should not be held hostage to even legitimate profit-seeking demands of private investors.

In brief, the nation should be investing in the deployment of fiber, powerline, wireless, and satellite communications technologies. The combination of these technologies would ensure robust and ready communications services in case of a national emergency. What's more, these technologies are readily available for roll out, as we will detail below.

OPTICAL FIBER

The most promising single technology that could deliver advanced telecommunications connectivity to homes and offices everywhere is optical fiber, a thin glass or plastic line designed to distribute light. Optical fiber is distinct from the electricity that distributes communications through copper telephone wires or coaxial cable. The light in optical fiber permits transmission of digital data over longer distances and at higher rates than other forms of communications.

Fiber optic products have been used for several decades in a variety of defense technologies designed for air, sea, ground, and space applications. During the high technology boom of the 1990s many privately held companies and public corporations built out vast fiber optic networks even as telecommunications companies beginning in the early 1990s began to upgrade their networks to incorporate fiber technology. Yet only one large U.S. company, Verizon, has extended optical fiber to the home.

The immediate reaction from Wall Street to Verizon's plans was pessimistic. Verizon's stock value in 2006 dropped and investors pressured the company to scale back deployment or abandon the investment in fiber to the home altogether. The reason: Investors saw little reason to back Verizon's expensive (\$23 billion) proposition.¹⁷

Nevermind that over time Verizon's emphasis on delivering video entertainment alongside other telecommunications services so the company could compete with cable is now increasingly viewed as smart forward-thinking investment strategy. Unfortunately, Verizon's service areas are largely densely populated urban areas, and Verizon's rural customers are not likely to get fiber anytime soon. Other telecommunications companies, including AT&T and smaller, regional players, have no plans to provide their customers with fiber optic service to the home.¹⁸ Again, the emphasis on market priorities, forward thinking or not, does not serve the goal of protecting Americans with the best communications service available in case of an emergency.

There are municipalities, however, that have deployed optical fiber networks with the expressed intent of improving the communications capability of emergency workers. One example is Arlington County, Virginia, just across the Potomac River from Washington, D.C. Arlington firefighters were the first to respond on September 11, 2001, when the Pentagon was attacked by terrorists. Beginning with its 10 fire stations in January 2002, by June 2002 all 40 county sites were connected to a fiber network. In 2005, Arlington extended the network to the nearby city of Alexandria, to facilitate inter-agency collaboration.¹⁹

These are the kind of public investments that federal, state, and local governments all need to make in tandem with the private sector to ensure that households and offices are all connected to the most readily available form of high-speed telecommunications. Ubiquitous broadband via fiber optics is the best first step that could be made by such a public/private partnership.

POWERLINE COMMUNICATION

Broadband over power lines, known as BPL by industry insiders, is a promising technology that would make use of the extensive electrical power grid infrastructure to communicate digital signals. BPL, however, still has some kinks to be worked out. Both the electric grid and the home create what engineers call a “noisy” environment. Every time a device turns on or off, a pop or click is introduced into the line.

Indeed, BPL has developed faster in Europe than in the United States due to differences in power system design philosophies. Large power grids transmit power at high voltages to reduce transmission losses, and transformers that are near the customer reduce the voltage. Because BPL signals cannot pass through transformers, repeaters must be attached to each transformer. In the United States, a small transformer typically services a single house or a small number of houses. In Europe, it is more common for a larger transformer to service up to 100 houses. Delivering BPL over the power grid of a typical U.S. city will require many more repeaters as compared to a typical European city.

Despite these challenges, BPL in the United States is on the rise, with about 6,000 BPL subscribers nationwide as of 2006.²⁰ According to the United Power Line Council, commercial deployments are up slightly, from six in 2005 to nine in 2007. Trial rates, however, have fallen from 35 in 2005 to 25 in 2007.²¹

An indication of a possible increase in BPL penetration, however, came in 2007 when DirecTV announced that it was getting in on the BPL market. In a deal with Current Group, DirecTV plans to provide BPL service in the Dallas-Fort Worth and Cincinnati areas with a potential for much broader rollout. Not to be out done, Oncor, a subsidiary of Dallas power company Energy Future Holdings Corporation—formerly TXU Corporation—has started to deliver BPL service and it recently passed 108,000 customer deployments, less than five percent of its goal.²²

The rise in BPL deployment can also be traced to steps the FCC took in 2006 to support the technology by reaffirming an earlier decision that BPL providers have the right to provide data access using power transmission lines so long as they do not interfere with existing radio service. Still, opponents of BPL, including the aviation industry and the amateur radio community, have continued to voice the strongest concerns over the issue of possible interference with radio communication,²³ though there is some dispute among experts over the degree to which electricity over BPL actually “leaks” and thus interferes with an electromagnetic wireless signal.

In a further boost, the FCC classified BPL-enabled Internet access as an information service, rather than a telecommunications service, in November 2006. According to the FCC, “The order places BPL-enabled Internet access service on an equal regulatory footing with other broadband services, such as cable modem service and DSL Internet access service.”²⁴ According to Joe Marsilio, president and CEO of BPL equipment maker and integrator MainNet Powerline Inc., 70 percent to 80 percent of the nation’s electrical grid will be equipped with BPL in five to eight years.²⁵

This kind of rollout of BPL services, however, will not occur without a coherent policy advanced by those federal agencies responsible for keeping America competitive and secure. BPL could easily become the second ubiquitous source of broadband to all houses and offices with a plug. With only a few technology hurdles to clear, and with FCC regulatory clearance already evident, BPL through a public/private partnership could become available swiftly.

WIRELESS BROADBAND

As anyone who has attempted to carry on cell phone conversations in New York or rural America will attest, reliance on the most prevalent wireless technology in America would be misplaced.²⁶ Cell phones are no less ubiquitous in big American cities than they are in London or Taipei or Toronto,

but somehow cell phones seem much more reliable in other countries.

Coverage problems in the United States result from the lack of cell phone infrastructure—towers and repeaters—necessary to sustain a large number of users in the variety of locations. The infrastructure problems are directly tied to two factors. First, the costs to build that infrastructure at present outweigh the commercial benefit, which is the profit the telecommunications companies and their shareholders think they can realize. Second, because cell phone service is seen only as a commercial need, there is little public will to assist in supporting the cost of this infrastructure development by allowing, mandating, or helping to finance the build-out of towers and repeaters.

Coverage problems also result from the limited propagation characteristics of the spectrum set aside for cellular service. Most cell phone use in the United States is based on dated technology.²⁷ Advanced digital Internet protocols make possible voice, data, and video communications over mobile networks. Third-Generation or 3G broadband has been deployed effectively in the United Kingdom, Germany, Japan, and other countries, but the United States lags behind.²⁸

The creation of a next generation wireless broadband network is an important public policy goal. The public safety benefits of reaching this goal justify significant federal funding to subsidize the development of such a network. One proposal is that the funding of a 3G public safety network could come by redirecting the billions of dollars designated to the federal government's wireless network project—estimated between \$5 billion to \$10 billion—and which will only serve a limited number of federal agencies.²⁹

The focus, however, should not be on any one technology, but rather on the full funding of a public safety network that utilizes wired and wireless infrastructure. The establishment of a public safety network can serve as a strong starting point for the development of a next generation network for com-

The emphasis on market priorities does not serve the goal of protecting Americans with the best communications service available in case of an emergency.

mercial purposes. A public safety network, however, should not be held hostage to commercial interests.

Federal allocation of spectrum must be revised to allow for the deployment of advanced wireless technologies. Licenses for all current analog radio and television broadcasting must be revoked, after which at least 25 percent of this spectrum should be set aside for public safety purposes, and half of the “vacant” spectrum should be reserved for temporary experimental applications with a priority placed on those applications that serve public safety, health care, or educational institutions.

WI-FI AND WI-MAX

Wi-Fi is a digital wireless communications technology. The brand is owned by the Wi-Fi Alliance, a consortium of companies that have agreed to a set of interoperable products based on a standard (802.11) set by the Institute of Electrical and Electronics Engineers. Though the Wi-Fi Alliance apparently originally intended the name to mean “Wireless Fidelity,” later statements from the consortium suggest the name is not an acronym or abbreviation.

Wi-Max is an acronym for “Worldwide Interoperability for Microwave Access.” This was adopted by the Wi-Max Forum in 2001. Wi-Max adheres to the so called IEEE 802.16 standard and allows for higher speed networking across much wider geographic

distance than is currently possible with Wi-Fi. Both Wi-Fi and Wi-Max in the United States face the technical challenges of limited spectrum allocation, particularly when compared with Europe.

As of mid-2007 there were over 400 counties and municipalities with wireless networks. These networks are used for applications ranging from reading meters to managing traffic and providing Internet access. Most municipalities contract with private companies to build and operate the network, and understandably the private industry is primarily concerned about profit. Therefore, in addition to the technical challenges in the United States, there are substantial difficulties with the business model.

Because of both the technical and business challenges, large-scale municipal wireless projects are flopping in big cities all across the United States. The problems arising in Houston, Chicago, St. Louis, Philadelphia, and San Francisco are for the most part very similar: the infrastructure (nodes and towers) was not in place, and when private companies were contracted to build the infrastructure, raising public money was difficult. Plans to migrate to public from private service were complicated by the fact that the slower and less reliable Wi-Fi connections are not able to compete effectively against incumbent wired (cable or DSL) Internet providers. As one reporter put it:

This summer was hard on urban Wi-Fi. Exhibit A: the extreme corporate shake-up at Earthlink, one of the biggest names in municipal wireless. In the same few days, the Atlanta-based Internet provider abandoned its much-heralded proposal to build San Francisco's wireless network, faced a \$5 million fine from Houston for missing a contractual deadline in rolling out that city's network, and announced it would shed some 900 jobs—half of its staff—including the company's head of municipal Wi-Fi. In St. Louis, a \$12 million plan stalled out this summer when AT&T and the city couldn't

untangle an electricity snarl... That plan is on hold indefinitely. With these signs of the industry buckling, Chicago officials backed off their plans to install a city network after failing to reach an agreement with either of the competing wireless providers.³⁰

The success stories of municipal Wi-Fi come from small towns. In St. Cloud, Florida, a truly city-wide municipal Wi-Fi network exists at no cost to residents. Mountain View, California has a citywide wireless network owned by Google with free service to residents. Both these networks operate over relatively small geographic areas: Mountain View is 14 square miles; St. Cloud is 12 square miles. Of the 400-plus American cities and counties attempting municipal Wi-Fi, most cannot offer it for free. There are currently only 92 cities or towns with active municipal Wi-Fi networks.³¹

The telecommunications industry nonetheless argues that the involvement of municipalities creates unfair competition for private organizations because of their ability to use public assets. The industry also argues that municipal governments do not have the necessary expertise to operate or maintain the technology and anyway should not be “picking winners” in a competition among technological alternatives.³²

Preoccupation with these industry concerns largely obscures the needs of public safety and emergency response. While neither Wi-Fi nor Wi-Max will address all the communication needs of local communities, the establishment of these systems can help fill in the deployment gaps and assist in providing the important redundancy demands of emergency communication. Fixed microwave wireless communication systems can also help fill in critical gaps.³³ The real problem is the tendency to look for easy answers rather than implement comprehensive solutions that should include Wi-Fi and Wi-Max. Federal leadership is needed to push forward a rationale for public investment that puts a priority on safety and emergency response.

SATELLITE BROADBAND

Satellites in geostationary orbit can relay Internet speeds of about 0.5 megabits per second to the user. But satellite broadband typically allows for only 80 kilobits per second from the user. In many rural areas this is a substantial increase over what is typically available. Although DirecTV and a few others have invested in making satellite broadband service a commercial competitor, it suffers from serious competitive disadvantages. Bad weather and sunspot activity can cause unreliable signals and dropouts. Applications such as virtual private networks and voice over Internet protocol, or Internet telephony, are discouraged or unsupported. And most satellite Internet providers abide by a Fair Access Policy, limiting a user's activity, usually to around 200 megabits per day.

Perhaps the greatest commercial disadvantage, however, may be the delay that results from the 44,000 miles a signal would need to travel from the user to the satellite company. This delay results in a connection latency of 500 to 700 ms, as compared with a latency of 150 to 200 ms typical for terrestrial Internet service providers.

Still, new technology has decreased the weight and size of satellite antennae and receivers, which combined with computer tracking devices makes it easier to send and locate satellite signals. And perhaps the biggest advantage of satellite broadband, particularly for emergency use, is that it can be established very quickly on a mobile unit that can avoid an attack or be rushed to the scene of a natural disaster. Fixed towers and telecommunications conduits necessary for wired or terrestrial wireless services are much more vulnerable to attack or natural disasters.³⁴

All these communications technologies—satellite broadband, Wi-Fi and Wi-Max, wireless broadband, power-line communications, and optical fiber networks—are available for local, state, and national government to warn and protect citizens. It is not a matter of choosing one or the other, but intelligently investing in all these technologies and engaging in research to develop more. Government

protection of the U.S. telecommunications industry should take the form of ensuring that industry is protected in case of an attack or natural disaster, it should not take the form of protecting industry profit at the expense of national security. America needs a robust communications system for emergencies the nation will surely face in the future.

WHERE ADVANCED ICT INFRASTRUCTURE SHOULD BE DEPLOYED

All government offices, health care centers, primary and secondary schools, military, police and fire, and emergency responders need access to advanced information and communications technology to prepare for and respond effectively to natural disasters and terrorist attacks. Federal and state governments may bicker over their relative access to advanced ICT, but there is little disagreement over the need for access. Similarly, while there are disputes on the edges there is a general consensus that police, fire, and emergency responders need this access.

But there are other institutions in this country that require ubiquitous broadband access in order to help our citizens in times of crisis, the two most critical sectors being educational and health care institutions.

Health Care Centers

Health care centers face extraordinary burdens during and after emergencies. The victims of natural disasters or other catastrophes require medical attention, as do the emergency responders who risk their lives. The ability to diagnose and monitor patients, to access patient records, and to communicate with pharmacists is increasingly dependent upon reliable communications systems within and beyond the hospital.

The absence of robust and redundant communications systems in our community health care facilities puts at risk not only patients but those who risk their lives to keep the rest of us from hav-

ing to enter the hospital. In addition, advanced telecommunications systems have proven to be effective in providing access to medical expertise even over great distances.

A cardiac patient in a small military hospital in Guam, for example, was able to undergo a life-saving heart operation supervised by an expert doctor located 3,500 miles away at Tripler Army Medical Center in Honolulu. The surgery was relatively routine for Dr. Benjamin Berg, who was able to dictate the procedure to a less experienced colleague, monitoring every move and heartbeat with a high-resolution video camera and instant sensor gathering data from the catheter as it was slid carefully into the right chamber of the patient's heart.

"The real-time information requires a continuous broadband connection," Berg said. "The delay in the transmission of data about pressure inside the heart would be unacceptable."³⁵ Imagine doctors being able to help patients remotely as the health care centers in New York and the Gulf Coast were inundated.³⁶

The example cited above of the surgeon in Honolulu supervising an operation in Guam is but one of the remote care practices engaged in by the Veterans Administration system. The VA also works with the Alaska Federal Healthcare Access Network, which links nearly 250 sites including military installations, Alaska Native health facilities, regional hospitals, small village clinics, and state of Alaska public health nursing stations to provide various healthcare services using high-speed broadband services including satellite broadband.

A VA study of a remote monitoring program demonstrated a 40 percent cut in emergency room visits and a 63 percent reduction in hospital admissions. A separate Penn State University study estimated that remote home health monitoring for diabetes patients cut costs for hospital care by 69 percent. According to Jon Linkous of the American Telemedicine Association, "Broadband Internet access to hospitals is becoming a critical tool in the delivery of medical services."³⁷

In addition to providing the communications infrastructure to local health care facilities, it is vital to increase support for both the National Institutes of Health and the Center for Disease Control. NIH has long demonstrated its importance in emergency and disaster readiness. One notable program is the University of California, San Diego and the California Institute for Telecommunications and Information Technology's \$4 million WIISARD (Wireless Internet Information System for Medical Response in Disasters) project, which is funded by NIH's National Library of Medicine.

The WIISARD project allowed the San Diego Metropolitan Medical Strike Team to bring together scientists and engineers from the California Institute for Telecommunications and Information Technology with local and state police, SWAT, fire, HazMat, and other first responders. In a simulation in 2005, the team was able to test the prototype of a video system that allows medical personnel to view a 3D virtual environment generated by a live video stream.

In another new technology demonstration by the WIISARD project, first responders were provided wireless personal digital assistants, or PDAs, outfitted with software to help them keep track of victims' locations and triage status, capturing important medical data at the point of triage and transmitted that immediately back to hospitals and a command center using a Wi-Fi network. According to Jacobs School of Engineering computer science and engineering professor Bill Griswold, San Diego's Metropolitan Medical Strike Team "has realized that law enforcement is an integral part of medical disaster response, and to better coordinate that, they anticipate that technologies like this can be useful in communicating from law enforcement to medical responders without distracting law enforcement from their duties."

Griswold adds that "we've also had some interest from SWAT officials because these technologies would allow SWAT teams to communicate information silently back to their commanders. Currently they have to use hand signals or radios,

Broadband Internet access to hospitals is becoming a critical tool in the delivery of medical services.

both of which put them at risk from exposing their positions.” Continued NIH funding to support this work is critical in keeping the nation safe and prepared for emergencies.³⁸

Similarly, but on a national scale, the Center for Disease Control and Prevention is an essential health care institution in emergencies, particularly in an age of biological weapons and biohazards that spread as a result of natural disasters. Whether it is containing the threat of anthrax or limiting the spread of waterborne human disease, it is essential for the CDC to have effective communications capability in the first hours of an emergency.³⁹

Educational Institutions

In 1957 America rested assured of its status as a singular world power, convinced of her superiority on every front after the victory of World War II, after the development and detonation of an atom bomb, and after the resurgence of the economy that followed the Great Depression and allowed the United States to contribute to the rebuilding of Europe. America could finally rest, and rest easy. And then, in October of that year, America’s rest was rudely interrupted by Sputnik.

The Soviet Union’s launch of an orbiting satellite haunted the American dreamscape with the sudden threat of communist missiles raining down from the skies, which sent school children under their desks to duck and cover. The Director of Development for

the Army Ballistic Missile Agency at the time, German rocket scientist Werner von Braun, testified before a subcommittee of the House Committee on Education and Labor:

Modern defense programs... are the most complex and costly, I suppose, in the history of man. Their development involves all the physical sciences, the most advanced technology, abstruse mathematics and new levels of industrial engineering and production. This... require[s] a new kind of soldier, who may one day be memorialized as the man with the slide rule... It is vital to the national interest that we increase the output of scientific and technical personnel.⁴⁰

Sputnik’s wake-up call led directly to the establishment of the Defense Advanced Research Projects Agency, or DARPA, which is credited for inventing the Internet. It also led directly to the passage of the 1958 National Defense Education Act. The NDEA allocated approximately \$1 billion in funds to supporting research and education in the sciences through 1962.⁴¹ The connection between education and defense could not be clearer.

Of course, educational institutions must have robust communications systems to warn and protect teachers and students. But to focus solely on American schools because they might be targets holding our children, our most valuable assets, would be to miss the lessons of the past. Our schools, whether at the elementary or at the graduate school level, must have the most advanced information technologies available if we are to develop the minds we will need to protect ourselves and find solutions to the various complex challenges in an increasingly complex world.

U.S. students and teachers must have ready access to the most advanced information technologies available. To deny this access because a government investment may challenge the interests of private corporations misses the larger point that not doing so will rob those corporations of the very minds they need to stay competitive. To

deny access to this technology may rob the nation of the resources it needs to save itself.

The importance of making advanced communications technology available to schools and students has been the subject of hundreds of reports over the past 50 years. Information technology leaders in higher education were actively engaged in planning and deploying the networks that led to the formation of what many think of as the original Internet, the NSFnet of the late 1980s, along with successful efforts to generate congressional support for scientific and academic networks, leading to the High Performance Computing Act of 1991, and the National LambdaRail effort to build an all-optical, facilities-based network for leading edge science and research.

The value of advanced broadband infrastructure is apparent in fields such as astronomy and genomics, but e-learning has barely scratched the surface of its potential.⁴² Students, particularly those who are not living at school, continue to have difficulty accessing broadband service. Undeterred, conservatives in the telecommunications industry continue to attack the Universal Service Fund program established by the 1996 Telecommunications Act, and have sought to undermine its effectiveness since its inception.

Yet the effectiveness of this program is undeniable. In 1998, at the beginning of the implementation of the USF program, only 14 percent of public school instructional classrooms were connected to the Internet; as of 2003, classroom Internet access was at 93 percent.

Nearly all public library outlets today are now able to offer some Internet access. Yet in each funding year since 1998, requests for E-Rate discounts vastly exceed the \$2.25 billion made available. Despite the clear need and success of Universal Service, the Bush appointees at the FCC have threatened support for the fund by excluding cable companies providing advanced telecommunication services from the requirement of a universal service contribution.

What's more, in 2004 the FCC suspended the E-Rate program for three months. The ostensible

reason: The FCC determined that the Antideficiency Act, which bars federal agencies from obligating funds without adequate cash on hand to cover those obligations, applied to the E-Rate.

The Universal Service Fund subsidizes the schools and libraries, the poor (Lifeline and Link-Up), rural telecommunications services, or telemedicine applications. When the Bush administration limits contributions and stalls funding it is heading in exactly the wrong direction. All Americans should have access to advanced telecommunications services whether they are poor, living in high-cost rural or urban areas, or living on fixed incomes.

Citizens remain our first line of defense and response in a natural disaster. If Americans are not connected, deployment will make little difference. USF support for advanced telecommunications services are clearly needed if all Americans are to be connected. A renewed commitment and a national broadband policy that puts universal access at the top of the list are past due.

CONCLUSION

The United States needs to move forward in a coherent fashion to deploy advanced telecommunications infrastructure, but not because we want to be number one. We have vulnerabilities at home that need to be addressed with some urgency. The possibilities resulting from the synthesis of powerful networks, computers, and databases have been the subject of a variety of blue ribbon panels, most notably the U.S. National Science Foundation report on cyberinfrastructure in 2003.⁴³ Five years later another panel is in order, with recommendations ready for a new administration and a new Congress.

The first work of such a panel should be to get accurate information on the deployment and capability of the various communications networks now operating in the United States. This paper has discussed a range of basic principles to meet the ends of national security and response to natural disasters. Those principles include:

- Robust networks capable of symmetrical speeds of 10 Gbps
- Redundancy
- Interoperability
- Network neutrality

We have a wide range of technologies available to communicate effectively. We should not choose between satellite broadband, Wi-Fi and Wi-Max, wireless broadband, power-line communications, and optical fiber networks—all of these technologies should be invested in along with new developing technologies to protect our defense and emergency needs at home. Because our citizens are our first line

of defense or response, we need to make a commitment to universal service regarding advanced telecommunications services for all Americans.

As President Eisenhower said in 1955, “Our nation is sustained by free communication of thought and by easy transportation of people and goods.” Our dependence on communications systems makes them more critical now than ever before. And as we pulled together and committed to the development of highways, satellites, and schools to win the Cold War, we must pull together now. **sp**

Mark Lloyd is Vice President for Strategic Initiatives, Leadership Council on Civil Rights.

NOTES

- 1 “Promoting Innovation and Competitiveness, President Bush’s Technology Agenda,” available at http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap4.html.
- 2 Mark Lloyd, “Raise the Bar on Broadband” (Washington: Center for American Progress, 2007),” available at <http://www.americanprogress.org/issues/2007/07/broadband.html>; and “Assessing Broadband in America: OECD and ITIF Broadband Rankings,” April 24, 2007, available at <http://www.itif.org/index.php?id=57>.
- 3 Leila Abboud, “How France Became A Leader in Offering Faster Broadband,” Wall Street Journal, March 28, 2006, available at http://online.wsj.com/public/article/SB114351413029509718-W1Q0hKioxOdz1Bs_6RCB7hQibg_20070328.html; “Successful Broadband Program Completed Ahead of Schedule,” Bell Canada Enterprises, June 29, 2006, available at <http://www.bce.ca/en/news/releases/aliant/2006/06/29/73706.html>.
- 4 CNN transcript of Vice President Al Gore’s remarks, Dec. 14, 1992, at the Little Rock Economic Summit, in a conversation with AT&T CEO Robert Allen; also cited in Charles Lewis, et al, *The Buying of the President* (New York: Avon Books, 1996), pp. 61–65.
- 5 Testimony of Craig E. Moffett, Vice President and Senior Analyst- Sanford C. Bernstein and Co., LLC, Before the Subcommittee on Communications, United States Senate, March 14, 2006, available at <http://commerce.senate.gov/pdf/moffett-031406.pdf> (Craig Moffett of Bernstein Research writes “In 60% of the country, there are simply no new networks on the horizon, and the existing infrastructure from the telcos—DSL running at speeds of just 1.5Mbps or so—simply won’t be adequate to be considered “broadband” in five years or so.”).
- 6 Richard F. Weingroff, “Federal-Aid Highway Act of 1956: Creating the Interstate System,” U.S.Department of Transportation-Federal Highway Administration, Summer 1996, Vol. 60: No. 1, available at <http://www.tfhrc.gov/pubrds/summer96/p96su10.htm>.
- 7 The National Commission on Terrorist Attacks Upon the United States, “9-11 Commission Report,” July 22, 2004, “The inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem,” available at http://www.9-11commission.gov/report/911Report_Ch12.htm. See also “Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks,” June 8, 2007, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-107A1.doc; “U.S. not ‘well-prepared’ for terrorism,” CNN, December 5, 2005 at <http://www.cnn.com/2005/US/12/04/911.commission/index.html#11>; Panel to issue report critical of federal security response: 9/11 Commission report card at http://i.a.cnn.net/cnn/2005/images/12/05/2005-12-05_report.pdf; Declan McCullagh, “Homeland Security flunks cybersecurity prep test,” CNET News.com, May 26, 2005, (http://news.com.com/Homeland+Security+flunks+cybersecurity+prep+test/2100-7348_3-5722227.html) (Agency’s lackluster efforts to guard against Internet attacks may leave the U.S. “unprepared” for emergencies, federal auditors say.); Eric Lipton, “Efforts by Coast Guard For Security Fall Short,” *The New York Times*, NYT, December 30, 2006, available at <http://select.nytimes.com/search/restricted/article?res=F40710FF3D540C738FDDAB0994DE404482> (“The communications, boat tracking and surveillance equipment rarely lives up to its promised capacity; for the largest systems, work is far behind schedule and over budget. Unlike the relatively unified command over the nation’s skies, control of the waterways and coasts is divided among at least 15 federal agencies, which sometimes act more like rivals than partners.”).
- 8 Statement of Adam D. Thierer before Senate Committee on Commerce, Science and Transportation, April 8, 2004 at <http://www.cato.org/testimony/ct-040428.html>.
- 9 The National Commission on Terrorist Attacks Upon the United States, *Ibid.*, at http://www.9-11commission.gov/report/911Report_Ch12.htm (“The attacks on 9/11 demonstrated that even the most robust emergency response capabilities can be overwhelmed if an attack is large enough. Team-work, collaboration, and cooperation at an incident site are critical to a successful response. Key decision-makers who are represented at the incident command level help to ensure an effective response, the efficient use of resources, and responder safety. Regular joint training at all levels is, moreover, essential to ensuring close coordination during an actual incident. Recommendation: Emergency response agencies nationwide should adopt the Incident Command System (ICS).When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command.”).

- 10 National Cooperative Highway Research Program, "The Interstate and National Highway System—A Brief History and Lessons Learned," June 13, 2006 at <http://www.interstate50th.org/docs/techmemo1.pdf>.
- 11 National Communications System, "Background and History of the NCS," at <http://www.ncs.gov/about.html>.
- 12 David C. Walsh, "Inter-Agency Communications Systems Remain Uncoordinated," *National Defense*, January 2006, at <http://www.nationaldefensemagazine.org/issues/2006/jan/inter-agency.htm>.
- 13 Bruce Meyerson, "Katrina Rescuers Improvise Communications," Associated Press, September 2, 2005 at http://www.iridium.com/about/press/pdf/1-16197134_Eprint.pdf.
- 14 John Eggerton, "Katrina Spotlights Spectrum Issue," *Broadcasting & Cable*, September 2, 2005, available at <http://www.broadcastingcable.com/article/CA6253687?display=Breaking+News&referral=SUPP>.
- 15 See Timothy Roemer comments "Lessons of Katrina: Critical Infrastructure, Preparedness and Homeland Security" Center for American Progress conference at <http://www.americanprogress.org/kf/katrina%20infra%20conference%20transcripts.pdf>.
- 16 U.S. Department of Homeland Security, "DHS Releases Nationwide Interoperable Communications Assessment," January 3, 2007, available at http://www.dhs.gov/xnews/releases/pr_1167843848098.shtm.
- 17 Jessica Seid, "Too early to hang up on Verizon?," CNN/Money Stock Spotlight, October 21, 2005 at http://money.cnn.com/2005/10/21/markets/spotlight/spotlight_vz/index.htm. "The entire telecom industry has taken a hit this year but Baby Bell Verizon Communications has really taken it on the chin. Shares of the New York-based telecommunications giant have tumbled 28 percent this year, making Verizon (Research) the second worst performing stock in the Dow industrials. But investors are also worried about high capital spending as Verizon gets set to launch its own video service to better compete against cable."
- 18 Michael Morisy, "Can AT&T's VDSL compete in a fiber world?," Telecom.com, Oct. 9, 2007 at http://searchtelecom.techtarget.com/originalContent/0,289142,sid103_gci1275983,00.html.
- 19 Cisco Systems Incorporated, "County Government Capitalizes on Network to Improve Public Safety and Quality of Life," at http://www.cisco.com/web/strategy/docs/gov/CS_ArlingtonCounty.pdf.
- 20 Annie Lindstrom, "Is BPL Gaining Momentum- Again?" XChangeMag.com, December 27, 2006, at <http://www.xchangemag.com/articles/501/6ch201042153728.html>.
- 21 UPLC Deployment Map, UPLC.org, Accessed September 27, 2007.
- 22 BPL Today, "Oncor (TXU) BPL deployment passes 108,000 customers," BPLToday.com, September 25, 2007, at <http://www.bpltoday.com/members/1236.cfm>.
- 23 Wayne Rash, "FCC Supports Broadband Over Powerlines," EWeek.com, August 3, 2006, available at <http://www.eweek.com/article2/0,1759,1998647,00.asp>.
- 24 FCC, "FCC Classifies Broadband Over Power Line-Enabled Internet Access as 'Information Service.'" news release, November 3, 2006, available at http://fall-foss.fcc.gov/edocs_public/attachmatch/DOC-268331A1.doc.
- 25 Annie Lindstrom, "Is BPL Gaining Momentum- Again?" XChangeMag.com, December 27, 2006, available at <http://www.xchangemag.com/articles/501/6ch201042153728.html>.
- 26 Li Yuan, "Why You Still Can't Hear Me Now," *The Wall Street Journal*, June 13, 2005 available at http://www.ocreger.com/ocr/2005/06/13/sections/business/business/article_556623.php; Sarmad Ali, "The 10 Biggest Problems With Wireless and How to Fix Them," *The Wall Street Journal*, October 23, 2006, available at <http://online.wsj.com/article/SB116120231104396746.html>.
- 27 FCC Consumer Advisory, Analog-to-Digital Transition for Wireless Telephone Service at <http://www.fcc.gov/cgb/consumerfacts/analogcellphone.html>.
- 28 Ben Charny, "U.S. carriers pick up the 3G pace," ZDNet News, Mar 22, 2004, available at http://news.zdnet.com/2100-3513_22-5176504.html.
- 29 The CTIA-sponsored roundtable report, "Toward A Next Generation Network for Public Safety Communications," available at http://www.silicon-flatirons.org/conferences/Hatfield_Weiser_PublicSafetyCommunications.pdf.
- 30 Chris Gaylord, "Municipal Wi-Fi Thrives- On a Small Scale," *Christian Science Monitor*, September 13, 2007, available at <http://www.csmonitor.com/2007/0913/p13s01-stct.html>.
- 31 Muniwireless, available at www.muniwireless.com.
- 32 Francois Bar and Namkee Park, "Municipal Wi-Fi Networks: The Goals, Practices, and Policy Implications of the U.S. Case," *Communications & Strategies*, 61 (1) (2006): 107–125.
- 33 "Milpitas, California, Deploys Metro-Scale Wi-Fi Public Safety Network from Tropos Networks," *Business Wire*, June 8, 2004, available at <http://www.govtech.com/whatsnext/assets/Brochure-Fixed%20Wireless%20for%20Public%20Safety.pdf>.
- 34 "SIA First Responder's Guide to Satellite Communications," Satellite Industry Association, available at <http://www.sia.org/guide.pdf>.
- 35 John Borland and Jim Hu, "A life-saving technology," CNET News.com, July 26, 2004, available at http://news.com.com/Broadband+A+life-saving+technology/2009-1034_3-5261361.html.
- 36 Leonard A. Cole, "Asleep in the E.R.," *The New York Times*, June 10, 2007, available at <http://www.nytimes.com/2007/06/10/opinion/nyregionopinions/10NJcole.html?ex=1188619200&en=433c43e50935adc5&ei=5070>; Robert Davis, "Hospitals learn from Katrina," *USA Today*, January 23, 2006, available at http://www.usatoday.com/news/nation/2006-01-23-katrina-hospitals_x.htm.
- 37 "Advancing Healthcare Through Broadband: Opening Up a World of Possibilities," Internet Innovation, Wednesday, October 24, 2007, available at <http://www.internetinnovation.org/tabid/56/articleType/ArticleView/articleId/86/Default.aspx>.
- 38 "UCSD Researchers Test Wireless Technologies in Simulated Medical Disaster Response Drill," May 16, 2005, available at http://www.jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=384 and <http://www.bbwxchange.com/publications/newswires/page546-2252944.asp>.
- 39 Communicating in the First Hours, available at <http://www.bt.cdc.gov/firsthours/overview.asp>.
- 40 "Hearings Before a Subcommittee of the Committee on Education and Labor on H.R. 10381, H.R. 10278 (and Similar Bills) Relating to Educational Programs" (Part 3) United States Government Printing Office: 1958, 1309.
- 41 Roger Geiger, "Sputnik and the Academic Revolution" Conference paper from "Federal Support for University Research: Forty Years After the National Defense Education Act & the Establishment of NASA." available at <http://ishi.lib.berkeley.edu/cshe/ndea/geiger.html>.
- 42 "Broadband America—An Unrealized Vision," EDUCAUSE, July 2004, available at <http://www.educause.edu/ir/library/word/NET0409.doc>.
- 43 NSF Blue-Ribbon Advisory Panel, "Revolutionizing Science and Engineering Through Cyberinfrastructure: Report of the NSF Blue-Ribbon Advisory Panel on Cyberinfrastructure," the Directorate for Computer and Information Science and Engineering, NSF, January 2003, available at <http://www.cise.nsf.gov/sci/reports/toc.cfm>.