BROADBAND & TELEMEDICINE

As the United States focuses on overhauling its healthcare system, policymakers face a number of critical decisions regarding the role of telemedicine. The following policy recommendations, which stem from a paper authored by the Advanced Communications Law & Policy Institute at New York Law School titled “The Impact of Broadband on Telemedicine,” are offered to policymakers at all levels of government as they consider healthcare reform. These recommendations offer guidance for helping ensure that life-enhancing telemedicine services are made increasingly available to patients and caregivers across the country regardless of their geographic location.

Recommendations for meaningful policymaking include:

1. Insurance laws, particularly reimbursement mechanisms, should be updated to promote greater adoption and use of telemedicine services.

2. Modernize and harmonize privacy laws to ensure more robust adoption and use of telemedicine services by healthcare providers and patients.

3. Craft and implement security standards to ensure that telemedicine services are secure and confidential.

4. Create an efficient and uniform physician licensure system that allows and encourages doctors to use broadband-enabled telemedicine services in the treatment of patients regardless of geographic location.

5. Tort reform is needed to protect telemedicine practitioners from frivolous lawsuits and to encourage the continued adoption of broadband-enabled telemedicine devices and services.

6. A combination of targeted policymaking and public-private partnerships should be used to facilitate the deployment of broadband to unserved areas of the country and to educate consumers about the benefits of telemedicine.

7. Bolster the nation’s pro-investment regulatory framework for broadband in order to encourage continued innovation of networks and telemedicine technologies.
Policy Recommendation 1

* * * * *

Insurance laws, particularly reimbursement mechanisms, should be updated to promote greater adoption and use of telemedicine services.

A formidable barrier to the continued expansion of broadband-enabled telemedicine applications is an antiquated set of insurance laws that do not provide adequate economic incentives for healthcare providers to adopt and use these types of services. For example, most public and private health plans do not reimburse doctors for using telemedicine applications. Without a reimbursement scheme that compensates a doctor for both “real” and “virtual” medical consultations and procedures, the healthcare paradigm in this country will continue to be rooted in traditional face-to-face encounters and will not sufficiently migrate towards more efficient, ubiquitous, and affordable healthcare via broadband-enabled telemedicine.

Healthcare in the United States is financed by two streams of funding: 1) the collection of money for healthcare (e.g. insurance premiums and taxes), and 2) the reimbursement of health service providers for healthcare (e.g., money to doctors from insurance carriers or the government). Telemedicine cost issues are primarily concerned with the latter. The mechanics of most private health plans typically mirror those of government at both the state and federal level, especially on issues of reimbursement. Thus, it is vital for state and federal governments to take the lead by updating their reimbursement schemes to include the full spectrum of telemedicine services.

Government healthcare is largely disbursed via Medicare and Medicaid. Medicare is a single-payer program that covers some 42 million Americans—35.4 million senior citizens and 6.3 million people under age 65 with permanent disabilities. It is financed by federal income taxes, a payroll tax shared by employers and employees, and individual enrollee premiums. Medicaid, on the other hand, is operated at the state level and covers approximately 55 million low-income Americans. Medicaid programs are financed jointly by the states and federal government through taxes so that every dollar spent by a state on Medicaid is matched by the federal government by at least 100 percent.

Given the broad reach of these programs, Medicare and Medicaid account for substantial percentages of healthcare providers’ revenues. However, under the current reimbursement structure for these programs, many advanced telemedicine services generally are not reimbursable. As a result, healthcare providers often lack a financial incentive to adopt and use these types of services. Recent reforms signal a growing recognition of the value of telemedicine services.
Over the past few years, Medicare has expanded to include certain types of telemedicine and telehealth services. However, the scope of the new reimbursement structure is still limited. For example, Medicare will only pay for telemedicine services that are provided via video conference. Medicare has a much narrower and less inclusive view of in-home telemedicine; it does not cover in-home medical service provided via a telecommunications service. “Store and forward” services like teleradiology are covered but only certain certified healthcare facilities are eligible to provide Medicare-supported telemedicine services. Recently, Medicare announced a pilot program in Arizona and Utah that allows beneficiaries to maintain and manage EHRs. However, beneficiaries can only choose from among a limited list of participating EHR providers.

Medicare and Medicaid reforms vis-à-vis telemedicine are encouraging, but more can be done. For example, most reimbursements are given to telemedicine providers who serve rural areas. While telemedicine was originally developed, and is still primarily used, for the provision of healthcare to remote patients, these types of services are increasingly used in urban and suburban settings. Limiting reimbursement to rural telemedicine would slow the adoption and use of these services across the entire population. As Debbie Voyles of Texas Tech observes: “There are a lot of patients in inner-cities that have difficulty getting in to see a physician, but they’re excluded from reimbursement.” Unfortunately, policymaking cannot keep pace with technological innovation, as evidenced by the antiquated notions included in many insurance plans.

Reimbursement mechanisms must evolve with the healthcare system. This includes recognizing the increased use and effectiveness of telemedicine services and providing reimbursement mechanisms for them regardless of where and to whom the services are administered. Reforms adopted and implemented by the federal government will likely prod state governments and private insurers to follow suit. Moreover, private insurers should be encouraged to experiment with telemedicine reimbursement independent of federal or state reforms. Indeed, a handful of states require private insurers to provide some form of telemedicine reimbursement. Otherwise, the U.S. healthcare system will continue to bloat and will be unable to realize the potentially enormous cost-savings associated with broadband-enabled telemedicine services.

Policy Recommendation 2

Modernize and harmonize privacy laws to ensure more robust adoption and use of telemedicine services by healthcare providers and patients.

In addition to updating insurance laws, policymakers must also address a variety of legal issues that potentially block wider adoption of lifesaving telemedicine services. Foremost among these is privacy.
The security of personal health information is paramount to doctors and patients as more advanced telemedicine services and devices collect and transmit an increasingly large volume of medical data over the Internet. Although transferring personal health information electronically via e-mail or an EHR may be efficient, it also raises important issues regarding the confidentiality of patient data and the possibility of private medical information being illegally viewed or stolen by a third-party.\(^{14}\)

To date, many states have enacted laws of general applicability regarding the electronic transmission of health information. These laws were crafted in response to the mostly intrastate nature of many modern telemedicine services that have been launched. However, newer broadband-enabled telemedicine services allow for the transmission of health data in real-time manner across state lines and even international borders. Thus, the existence of a patchwork system of privacy standards forged to address intrastate services increases compliance costs in a borderless digital world and decreases the incentive for doctors to share data with healthcare providers in other states.

In order to resolve these discrepancies, policymakers should consider adopting a national framework for ensuring the privacy of interstate electronic health communications in the United States. This would improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of broadband-enabled telemedicine services and applications like EHRs and remote monitoring systems regardless of geographic location.\(^{15}\) Unfortunately, the current set of health privacy policies is out of date, which risks slowing the deployment and adoption of critical telemedicine tools.

In 1996, Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") to, among other things, streamline electronic medical record systems while protecting patients, improving healthcare efficiency, and reducing fraud and abuse.\(^{16}\) HIPAA requires healthcare providers, health plans, and business associates to adopt security and privacy standards for electronic communications, medical records, and medical transactions.\(^{17}\) Prior to HIPAA, a “comprehensive personal right to privacy in one's medical affairs did not exist.”\(^{18}\)

HIPAA, however, only addresses some of the privacy concerns related to the electronic transmission of health data. The HIPAA privacy component, which creates standards for maintaining the integrity of protected health information, is applied to information that is transmitted for healthcare operations, as well as financial or administrative purposes.\(^{19}\) Covered entities, which include all health plans, healthcare clearingshouses, and healthcare providers who conduct electronic healthcare transactions, are responsible for ensuring HIPAA compliance from their business associates who receive protected health information in the process of providing services to the covered entity.\(^{20}\) Yet the advent of more advanced broadband-enabled telemedicine services raises several privacy issues.
that are not typically encountered during conventional medical practice. These include:

► Telemedicine could reasonably be regarded as a healthcare operation and therefore fall under the "treatment, payment, or healthcare operations" categorization, which permits the use and disclosure of protected health information without patient consent.

► Teleconsultations may require additional non-clinical personnel (e.g., technicians, camera operators, etc.) who do not participate in traditional medical care but who nonetheless would be required to comply with all HIPAA regulations.

► In traditional medical care, providers typically have existing relationships with the medical specialists with whom they consult. However, when dealing with telemedicine, patients and their on-site medical providers often will not know which clinical and non-clinical personnel will be involved at the distant site. HIPAA does not directly address this situation.

Solutions to these privacy issues have been offered by a number of organizations. For example, Connecting for Health, an initiative supported by the Markle Foundation, recently issued a comprehensive Common Framework for Networked Personal Health Information ("Framework"), which offers solutions for many of these concerns. The Framework, which addresses privacy issues from both the consumer perspective and the technical perspective, defines a set of practices that can help protect personal information, enhance consumer participation in online personal health records, and is available free of charge on the Connecting for Health Website. Ultimately, the Framework seeks to empower individual users with full access to and control over personal medical information while providing them with a sense of absolute privacy in the management of their health information. A diverse array of healthcare-related groups, including consumer and privacy organizations (e.g. AARP), health insurers, healthcare providers, and technology companies (e.g. Dossia, Google, Intuit, Microsoft, and WebMD) have endorsed this framework.

Current telemedicine providers have used some of the strategies recommended by the Framework, such as the use of consent forms and patient releases. Lisa Gaudet of Northeast Health states that her programs requires “[all patients] to sign a release, which spells out the method that their data will be transmitted and viewed, the risks associated with that method, and the efforts we will take to protect their health related information.” Thus far, Northeast Health has not experienced any legal issues with data privacy or data security. Similarly, Oklahoma state law requires telemedicine providers like the Oklahoma State University Telemedicine Program to obtain the consent of every patient who is to receive telemedicine services by signing a Legal Consent Form. This allows patients to make informed decisions regarding the services that they are about to
receive. Moreover, in order to further ensure that privacy is not compromised, the Oklahoma State University Telemedicine Program does not record any of their telemedicine sessions. All procedures are completed in real time, just as they are in a local physician’s office.

Policymakers have the opportunity to update laws like HIPAA and harmonize conflicting state privacy laws in order to ensure the continued use of broadband-enabled telemedicine services. Decreasing the amount of privacy-related compliance costs would increase the incentive to adopt these new services and would increase the availability of effective and affordable healthcare.

**Policy Recommendation 3**

*Craft and implement security standards to ensure that telemedicine services are secure and confidential.*

As more and more healthcare services migrate online, questions regarding the security of sensitive health information being transmitted over the Internet have been raised. Many consumers worry about identity theft, spam, hacking, and other nefarious intrusions. Indeed, a recent study by Pew found that 75 percent of Internet users do not like giving out their credit card or personal information online. In the realm of healthcare, trust and security are at the center of the traditional doctor-patient relationship. As digital healthcare continues to evolve, it is essential that network and data security are addressed by telemedicine developers, users, and patients.

At the network level, security includes the development and implementation of standards for the secure transmission of health information. To date, the development of such standards has been slow. The continued prevalence of intrusive applications, like spam, frustrates users, decreases their enjoyment of the Web, and could delay further adoption of broadband-enabled telemedicine. Similarly, the increased use of Wi-Fi networks for in-home monitoring raises additional security issues. These types of networks tend to be less secure than wire-based ones, but their relative affordability and ability to interact with other wireless technologies (e.g., wireless sensors) have made them very attractive to researchers and patients. However, given the rising prominence of telemedicine services and their importance to the future of healthcare, private sector innovators have begun working together to address security issues.

For example, in April 2005, SafetySend formed a partnership with the American Association for Medical Transcription to create a private system that securely transmits personal health information. SafetySend’s service ([www.safetysend.com](http://www.safetysend.com)) includes solutions for organizations needing secure file transfer that comply with HIPAA privacy
standards. It also offers secure e-mail and fax components and is available for purchase by individuals for as little as $8 per month.

In addition, more secure wireless technologies continue to be developed. A team at the Rochester Institute of Technology has been working on integrating radio frequency identification (“RFID”) technology into cardiac sensor networks, which are used to remotely monitor a patient’s heartbeat pattern and blood pressure. This method will help transfer critical cardiologic information to doctors and hospitals, increasing the quality of diagnosis and reducing the need for medical supervision.

Many network security issues, however, may be solved as the bandwidth available to telemedicine providers increases. For example, according to Doug Power, Senior Consultant and Research Associate at the Regional Development Institute Northern Illinois University, which supports the Illinois Rural Health Network, robust fiber-optic broadband networks will allow telemedicine users and providers to send “secure transmission packets, via their own Virtual Private Network riding over the IRHN.” These types of dedicated networks will greatly enhance network security and increase consumer confidence in broadband-enabled telemedicine services.

Policy Recommendation 4

Create an efficient and uniform physician licensure system that allows and encourages doctors to use broadband-enabled telemedicine services in the treatment of patients regardless of geographic location.

The interstate (and global) nature of broadband-enabled telemedicine services is also challenging traditional notions of physician licensure, which currently limit doctors to practicing only in the states where they are licensed. The historical basis for state regulation of the practice of medicine is rooted in the Tenth Amendment, which delegates to states the power to, among other things, preserve the public health, welfare and safety of their residents. As a result, states have created licensing requirements and oversight boards to monitor health and medical practices across their territories. But in the modern healthcare marketplace, such laws are not reflective of the borderless nature of many telemedicine services. Thus, licensure laws that limit the practice of medicine to one state might unduly decrease the reach of telemedicine.

In 1997 and 2001, Telemedicine Reports to Congress identified licensure as a major barrier to the development and use of telemedicine services. Additional reports also recommended a more consistent framework to encourage interstate telemedicine. Thus far, incremental progress has been made as a number of alternative licensure models have been offered and considered. Many of these proposals are based on the notion of reciprocity, a system that permits one state to recognize a license in good standing that a
practitioner holds in another jurisdiction. These and other models limit the pool of doctors who are allowed to use telemedicine services in the treatment of patients regardless of geographic location. Having to comply with myriad licensure rules could delay treatment and deny a patient the services of a specialist who does not reside in an eligible state under the home state’s reciprocity rules.

One recommendation is for the adoption of a national licensure system for telemedicine. Such a system would expand the market for telemedicine, promote both the use and development of new technologies, and eliminate many of the legal and regulatory ambiguities that plague and constrain the present system. A national system would involve the issuance of a license based on a standard set of criteria for the practice of telemedicine throughout the United States. Disciplinary actions resulting from malpractice or other negligence would continue to be carried out at the state level subject to the national standards.

Outdated licensure systems represent a major obstacle to the expansion of telemedicine services. While telemedicine originated primarily as an intrastate service, broadband has removed physical state barriers and has the power to connect doctors and patients located anywhere in the world. As such, licensure models must be revised to provide for interstate (and eventually international) telemedicine services.

**Policy Recommendation 5**

*Tort reform is needed to protect telemedicine practitioners from frivolous lawsuits and to encourage the continued adoption of broadband-enabled telemedicine devices and services.*

The number of medical malpractice suits and settlements continues to increase each year. Indeed, the cost of medical malpractice torts had the largest growth among U.S. tort costs, totaling $28.7 billion in 2004, having increased an average of 11.7 percent annually since 1975. Telemedicine, by its nature an emerging and cutting-edge medical service, expands the reach of healthcare and thus increases the possibility of medical malpractice suits. As a result, many physicians are hesitant to adopt broadband-enabled telemedicine applications for fear of exposing themselves to greater liability. While doctors who use telemedicine services and tools negligently should certainly not be immune from lawsuits, policymakers should consider reforms that encourage the use of these services by updating tort laws to include telemedicine and telehealth.

As with licensure, tort laws are largely state-specific. Traditionally in tort cases, an important jurisdictional determination is where a tort occurred. Telemedicine complicates this determination because the doctor and patient are physically separated,
which muddies the traditional perception of the doctor-patient relationship. While federal tort law generally holds that the law of the patient’s home state controls, telemedicine injects some uncertainty because doctor and patient are connected only by a broadband connection. The possibility exists that a telemedicine provider could be exposed to a number of different tort laws should negligence occur.

The current uncertainty regarding tort law and telemedicine may discourage healthcare providers from adopting broadband-enabled telemedicine devices and services and using them to provide interstate care. Policymakers must recognize that broadband-enabled telemedicine has the potential to radically transform the U.S healthcare paradigm and that antiquated tort laws may potentially discourage physicians and other healthcare providers from using these tools to provide medical care to patients regardless of geographic location.

**Policy Recommendation 6**

*A combination of targeted policymaking and public-private partnerships should be used to facilitate the deployment of broadband to unserved areas of the country and to educate consumers about the benefits of telemedicine.*

The availability of robust broadband infrastructure is vitally important to the future of telemedicine. Devices and applications will become increasingly more bandwidth-intensive as they provide more sophisticated real-time monitoring, emergency alert, and other time-sensitive services. Thus, for telemedicine to be most effective, broadband must be made available to and adopted by users in every corner of the United States.

To date, broadband network owners have responded to growing demand for more bandwidth by investing billions of dollars in next-generation networks. Yet, for a wide variety of reasons, parts of the country remain unserved. Indeed, even though the FCC has found that “more than 99 percent of the country’s population lives in 99 percent of zip codes” in which there is at least one broadband provider, broadband remains relatively scarce in those zip codes with the lowest population density. As a result, the public and private sectors must work together on a solution for deploying advanced network infrastructure to unserved parts of the country and to educate the public about the profound impact that broadband services generally, and broadband-enabled telemedicine services specifically, can have on personal wellbeing. A number of tools are available.

First, as mentioned in Section 4, the federal government should continue to strategically use universal service funding to create unique programs and incentives for deploying advanced telemedicine infrastructure to unserved parts of the country. The FCC’s Rural Healthcare Pilot, which, among other things, promotes the creation of proprietary
broadband networks dedicated to the transmission of health-related services, has already been successful in spurring innovation and deployment of broadband across the country. Unique approaches like the Illinois Rural Health Net, the University of Virginia’s Southwest Virginia Alliance for Telemedicine, and various efforts in Alaska should be looked to as models for crafting solutions that fit specific local or state needs.

Second, local, state, and federal government should promote the use of public-private partnerships to bring broadband and broadband-enabled telemedicine services to rural, low-income, and other unserved consumers. The Connected Nation model, for example, has succeeded in spurring broadband availability and adoption in Kentucky and has been adopted in Minnesota, Ohio, Tennessee, and West Virginia. Additional efforts have succeeded in facilitating the deployment of robust telemedicine services to those most in need. University-based programs that are funded in part by federal grants have been especially successful to date. Similar approaches have led to breakthroughs in the fields of telepsychiatry and remote monitoring, and have helped to harmonize efforts by instituting a public-private standards-setting body for the HIT and telemedicine device sectors.

Third, these efforts must be coupled with efforts to raise awareness regarding the life-enhancing impacts of broadband-enabled telemedicine among a wider swath of patients and caregivers. A number of organizations that specialize in bringing broadband to specific segments of the population (e.g., Older Adults Technology Services for senior citizens and One Economy for low-income users) should be used as models for spurring demand for and use of these critical tools.

In the near term, special efforts should be made to bolster demand and use of broadband among senior citizens, as this large segment of the population stands to benefit the most from adopting broadband. A high-speed connection facilitates a wide range of social, economic, and health-related benefits for seniors, including a number of previously discusses telemedicine tools and service. Additional efforts might include education campaigns that target seniors, ensuring that online tools are designed in a senior-friendly way, and supporting local initiatives aimed at training seniors to use computers and the Internet.

Overall, a national commitment to incorporating telemedicine into a new healthcare paradigm is critical to transforming how medical care is provided in this country.

**Policy Recommendation 7**

*Bolster the nation’s pro-investment regulatory framework for broadband in order to encourage continued innovation of networks and telemedicine technologies.*
An essential prerequisite for cutting-edge innovation in the telemedicine industry is the wide availability of advanced broadband infrastructure. Indeed, many current telemedicine services rely on robust broadband connections to be effective. Over the next few years, most of the next-generation telemedicine applications and devices developed will be increasingly intertwined with broadband as the network becomes an ecosystem for more individualized medical care. Policymakers should thus bolster the pro-investment policies that have fostered an innovative broadband marketplace over the last decade in order to ensure that the telemedicine sector continues to thrive.

Investment in broadband network infrastructure, robust management and security protocols, and research and development are essential to ensuring continued innovation by developers of telemedicine services and applications. To this end, current economic conditions require careful policymaking that provides investors and innovators with certainty that their efforts will not be made in vain. Federal funding for the deployment of broadband via the recently adopted economic stimulus package will supplement USF funding in the short-term to support further network build-out to unserved parts of the country. In addition, funding that is allocated for expanding and promoting the use of EHRs and other health IT could also be used to bolster the adoption of broadband-enabled telemedicine services in hospitals, care centers, and other medical facilities across the country.

Additional vehicles for strategically targeting these funds to support the deployment of broadband networks to unserved areas and to spur further innovation in the telemedicine sector could include tax breaks to network owners, grants to support telemedicine-focused university programs and public-private initiatives, and innovative incentives for private entities to devote resources to the research and development of cutting-edge services.
Endnotes


4 Id.


6 Id.


8 Id.

9 Id.

10 Id.


12 Id.


17 Id.


19 Id.

20 Id.

21 Id.


Outgoing HHS Secretary Michael Leavitt recently articulated a set of guiding principles to bolster consumer privacy vis-à-vis digital health information. These included individual access to personal health information, openness and transparency, data integrity, and accountability. In addition, Secretary Leavitt also proposed the use of a label, modeled after the nutritional labels on food packaging, which would allow consumers to quickly compare personal health record products. See Press Release, Secretary Leavitt Announces New Principles, Tools to Protect Privacy, Encourage More Effective Use of Patient Information to Improve Care, Dec. 15, 2008, HHS, available at http://www.hhs.gov/news/press/2008pres/12/20081215a.html.


See Overcoming the Psychological Barriers to Telemedicine: Empowering Older Americans to Use Remote Health Monitoring Services, at p. 6, New Millennium Research Council (Feb. 2007), available at http://www.newmillenniumresearch.org/archive/Telemedicine_Report_022607.pdf (noting that as of Feb. 2007, such standards had yet to be developed).

Pew has found that “Spam continues to plague the internet as more Americans than ever say they are getting more spam than in the past.” However, users are increasingly adept at adopting tools to manage spam and similar applications. Indeed, Pew found that 71 percent of Internet users use spam filters on their emails accounts. See Deborah Fallows, Data Memo: The Volume of Spam is Growing in Americans’ Personal and Workplace Email Accounts, but Email Users are Less Bothered By It, at p. 1, Pew Internet & American Life Project (May 2007).


See, e.g., Telemedicine Licensure Report, The Center for Telemedicine Law & The Office for the Advancement of Telehealth (June 2003), available at ftp://ftp.hrsa.gov/telehealth/licensure.pdf (citing two examples: In 2002, when the House Commerce Committee inserted language in the Safety Net Legislation that expressed the Congressional interest in collaboration among regulatory boards to facilitate...
elimination of barriers to telehealth practice. (Healthcare Safety Net Amendments of 2002, Pub. L. No. 107-251, 116 Stat. 1621). This legislation was ultimately signed by the President. Similar language was included in the Senate version of the prescription drug legislation pending on Capitol Hill. (See S. 1, 108th Cong., 1st Sess. § 450H, 2003.).


50 FCC Broadband Stats - Jan. 2009 at p. 4 and Table 18 (noting that “High population density has a positive association with reports that high-speed subscribers are present, and low population density has an inverse association. For example, high-speed subscribers were reported to be present in more than 99% of the most densely populated Zip Codes and in 90% of Zip Codes with the lowest population densities.”).


Id. at 32-34 (discussing a number of ways to stimulate broadband demand among seniors).


The final stimulus bill includes $7.2 billion for broadband deployment to unserved and under-served areas of the country. However, mechanisms for identifying these areas and structuring disbursement of the funds were not included in the bill and will be developed by NTIA and the FCC. See Stephanie Condon, Stimulus Bill Includes $7.2 Billion for Broadband, Feb. 17, 2009, CNET NEWS.COM, available at http://news.cnet.com/8301-13578_3-10165726-38.html.

Health IT Stimulus. However, some experts have suggested that these funds should be spent elsewhere, as the current generation of EHRs are unlikely to lead to promised welfare gains. See Lisa Wangsness, Letter Highlights Hurdles in Digitizing Health Records, Jan. 1, 2009, BOSTON GLOBE.

For example, a number of executives working in the high-tech sector have recommended that any federal stimulus include tax credits for the investment in IT in order to promote continued innovation. See Janet Rae-Dupree, Innovation Should Mean More Jobs, Not Less, Jan. 4, 2009, N.Y. TIMES (noting that the plan “calls for a tax credit for companies that spend more than 80 percent of what they had been spending annually on information technology like computers and software.”).