INFORMATION

ABSTRACT:

The Information Industry is a viable, dynamic industry characterized by mergers and acquisitions. It faces many challenges, perhaps the most critical being the recent loss of venture capital. Despite the latest economic fluctuations, we project that demand will continue to expand. Whether this growth will match the 1990's levels will depend on consumer confidence and industry's innovation. The industry will continue to provide innovative products that will enable future growth in other sectors. While such high demand places a strain on the government's ability to influence the market, the Information Industry remains responsive to national security requirements.

COL Ibrahim Al-Hawawi Saudi Arabia
LTC Dominic Archibald USARNG
Ms. E. Rowe Campbell Defense Contract Management Agency
Lt Col Anthony Dominice USAF
Col Ivette Falto-Heck USAF
Mr. Frank Goss Dept. of Defense
CDR Floyd Hehe USN
Ms. Theresa Jackson Defense Information Systems Agency
Mr. Iftikhar Jamil Defense Threat Reduction Agency
Ms. Jackie Leitzel Dept. of the Air Force
Lt Col James McKinney USAF
LTC Ray Montford USA
COL Romeo Morrisey USA
Ms. Nancy Myrick Defense Logistics Agency
Ms. Pat Newman Dept. of Defense
CDR Edward Rackauskas USN
Lt Col Laura Shoaf USAF

COL (ret) Rich Altieri USA, faculty
Col Shelby Syckes USAF, faculty
Col Lynne Thompson USAF, faculty

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2001	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
2001 Industry Studies: Information	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Industrial College of the Armed Forces National Defense University Fort McNair Washington, DC 20319-5062**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**26**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

PLACES VISITED:

Domestic:
3COM Corporation, Santa Clara, CA
Agilent Technologies, Santa Clara, CA
Cisco Systems, San Jose, CA
COMCAST, Alexandria, VA
Exodus Communications, Santa Clara, CA
Foundry Networks, San Jose, CA
Information Technology Association of America, Rosslyn, VA
Intel Corporation, Santa Clara, CA
Handspring Incorporated, Mountain View, CA
McAfee Incorporated, Sunnyvale, CA
National infrastructure Protection Center, Washington, DC
Oracle Corporation, Redwood Shores, CA
Silicon Graphics Incorporated, Mountain View, CA
Software Information Industry Association, Washington, DC
Sun Microsystems, Santa Clara, CA
Teligent Incorporated, Herndon, VA
Verizon Communications, Washington, DC

International:
Eastern Seaboard Industrial Estate, Rayong, Thailand
Economic Development Board, Singapore
Hewlett Packard, Singapore
Infocomm Development Authority, Singapore
NTT Do Co Mo, Tokyo, Japan
SCI Systems Inc., Bangkok, Thailand
Shin Satellite, Bangkok, Thailand
Software Park, Bangkok, Thailand
Sony Media World, Tokyo, Japan
TECH Semiconductor Plant, Singapore
Telecommunications Association of Thailand, Bangkok, Thailand
U.S. Embassy, Thailand
Verizon Communications, Bangkok, Thailand

INTRODUCTION:

The Information Age affects the way we live, work and play. It is driving the Information Industry, as governments, businesses, and consumers increasingly demand communications, computers, and software for use in the Internet, intranets, and extranets. Information technology (IT) - enabled communication networks will soon become the predominant means of interaction between individuals, businesses, organizations, and governments. While the role of the Information Industry – meeting the need for IT products and services in the new economy – remains essentially the same, the industry itself continues to change. It is a viable, booming, dynamic industry characterized by mergers, acquisitions, and consolidations.

The Information Industry is difficult to distinguish from other industry sectors. Two factors contribute to this difficulty: 1) the rapid growth in the development of new IT and applications and 2) the integration of IT into virtually every sector of the new economy. This is evident in the recent turmoil in the stock market, apparently the result of the devaluation of Internet-based "dot-com" corporations. While the industry remains strong, this transient instability has slowed the growth of the industry from past double-digit levels.

Driven by high commercial and consumer demand, the industry will continue to provide innovative products and services that will enable future growth in other sectors. While such high demand places a strain on government's ability to influence the market, the Information Industry remains responsive to supporting the national security resource requirements. This study provides an overview of the Information Industry, discusses challenges and the outlook for the industry, and presents potential government goals and roles.

THE INDUSTRY DEFINED:

In 1997, the North America Industry Classification System (NAICS) replaced the traditional method of classification and defining industry sectors found in the old Standard Industrial Classification (SIC) Code. The information sector (sector 51) of the NAICS is composed of those establishments engaged in producing and distributing information and cultural products. They provide the means to transmit or distribute these products as well as data, or communications, and processing data. The main components of this sector include: Publishing industries (511), including software publishing; Motion picture and sound recording industries (512); Broadcasting and telecommunications industries (513); and Information and Data processing services industries (514).[1] To prevent duplication of coverage of motion picture and sound recording industries with the Media and Service Industry Study teams, we have omitted them from this analysis. This analysis of the Information Industry includes three general areas of IT products and services: 1) telecommunications, 2) computers and other information processing equipment, and 3) software. The analysis incorporates eight of the 52 Standard and Poor's Industry Surveys that most closely fit these three areas. These eight are:

- Communications Equipment[2]
- Computers: Commercial Services[3]

- Computers: Consumer Services and the Internet[4]
- Computers: Hardware[5]
- Computers: Networking[6]
- Computers: Software[7]
- Telecommunications: Wireless[8]
- Telecommunications: Wireline[9].

There is not a uniform structure to the Information Industry. Primarily, the communications equipment, computer hardware, computer networking, and telecommunications services sectors of the industry are oligopolies with a few companies dominating each (with the exception of wireline terminal equipment where there are many competitors). The computer commercial services, consumer services and the Internet, and software sectors generally are broadly based and very competitive (with a few exceptions such as operating systems). Innovation, research and development, and the demand to get new products to market quickly are the primary characteristics of the conduct of the overall Information Industry.

CURRENT CONDITION:

Continued growth characterizes the performance of the Information Industry. The Internet continues to lead the growth of the Information Industry, as well as the decline in the stock market. As of year-end 1999, about 186.2 million users worldwide accessed the Internet regularly, and International Data Corporation expects this number to soar to 502.5 million by 2003.[10] Clearly, the Internet is in a robust growth phase and t
his growth has pushed the capacity of existing networking infrastructure to its limits, resulting in some frustration among Internet users. A significant part of the growth forecast for Internet usage is coming from corporate demand. Businesses seek competitive advantage by better servicing and supporting their customers through their web sites or by linking with their suppliers through digital online exchanges – networks that provide business-to-business connections for online procurement. Businesses are also increasingly providing internal communications through intranets. During each growth phase of the computer hardware industry, the price for computing power has decreased, usability has increased, and the market has broadened.

Table 1 depicts the growth in the Information Industry. Figure 1 presents a graph of this growth. The S&P values are from a combination of the eight Standard and Poor's Industry Surveys listed above. The USITO values are from the US Industry and Trade Outlook 2000.[11]

	1994	1995	1996	1997	1998	1999
Total S&P	$442 B	$523 B	$529 B	$614 B	$688 B	$803 B
Percent Change		18.3	1.0	16.3	11.9	16.8
Total USITO	$456 B	$501 B	$557 B	$614 B	$685 B	$746 B
Percent Change		9.7	11.2	10.2	11.7	8.8

Table 1: Information Industry Growth (1999 $)

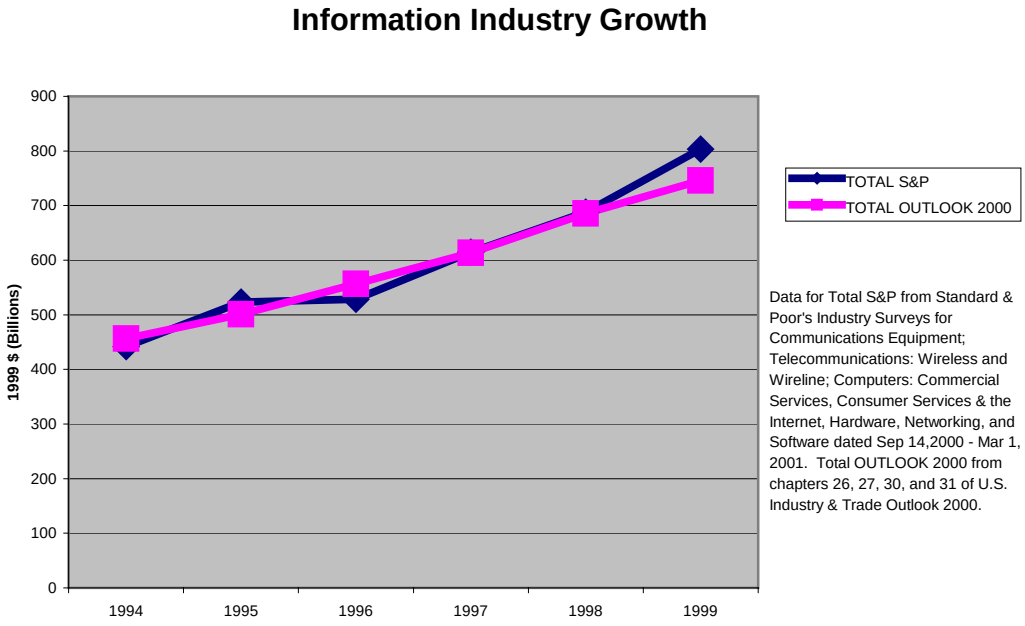

Figure 1 US Information Industry Growth

The Internet sector led the stock market decline that began in March 2000 with the publication of a cover story in Barron's that questioned the business models and viability of dozens of money-losing dot-coms. Individual companies' recent quarterly operating losses were subtracted from cash balances until the dollar reserves on their balance sheets reached zero. The article reported the number of months it would take for each of 207 dot-coms to burn through its cash. On the list, 51 companies were within a year of burnout.[12] Investors re-evaluated their choices and used more traditional valuation methods as a primary consideration. The values of dot-coms plummeted, and suddenly hundreds of companies and tens of millions of their employees and stockholders were quite poorer than they had been a year or two before. Reduced consumer confidence and the current malaise in the overall economy can be traced in many ways to the reversal in fortune of the dot-com sector. The Internet companies able to weather the storm will emerge stronger and wiser. Overall, the Information Industry continues to grow robustly to meet the increasing demands of government, businesses and consumers.

Projected to grow past $1.8 trillion by 2003, the Information Industry will continue to pace the growth in international trade, despite the transient effects of the current economic slowdown.[13] US Information Industry currently leads the international IT products and services market. As shown in Figure 2, the US Information Industry continues to run a trade deficit, mostly due to the computer equipment sector.[14]

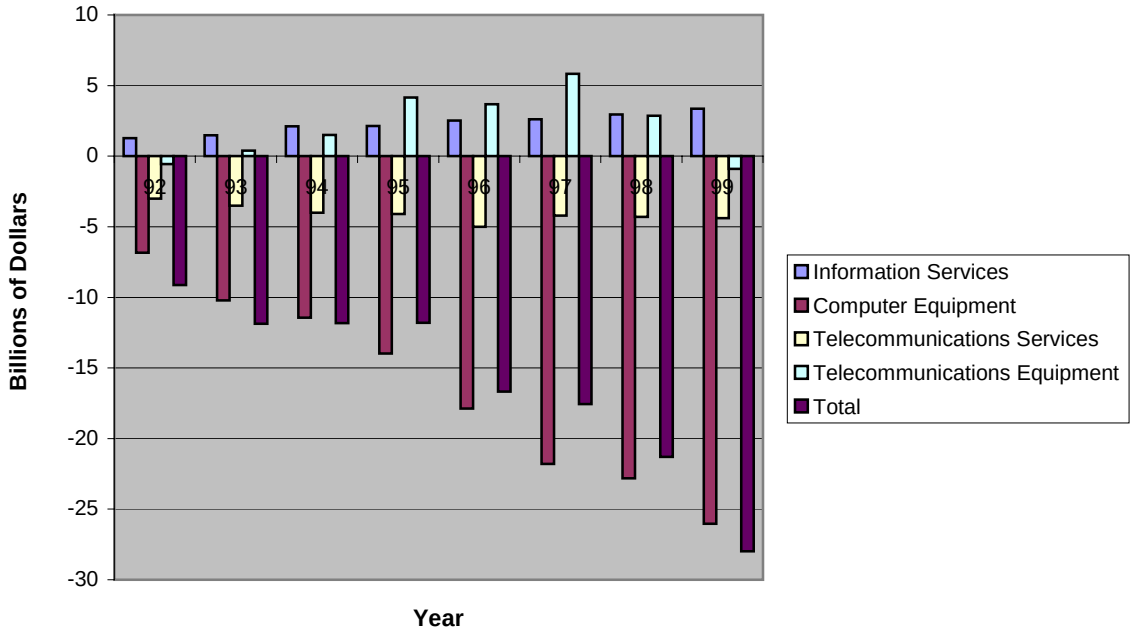

Figure 2. US Information Industry Trade Balances

With the economic incentives of the global market and the political push to expand trade in the name of democracy, US firms must be ensured equal competitive opportunity. To remain competitive and maintain the US' lead, these firms must be aware of the potential barriers to trade including:

- various forms of import fees such as tariffs, duties, or value added taxes
- non-tariff barriers such as conformity assessment, subsidies, licensing, and quotas
- regulation (or lack thereof) dealing with products and services, as well as intellectual property rights
- export control and licensing requirements

US participation in the World Trade Organization and its Information Technology Agreement mitigate some of the effects of the first three for businesses. However, US restrictive export controls and cumbersome licensing policies and procedures, in the name of national security, often contradict its own pro-trade efforts and the ability of American IT firms to compete equally in the global market.

CHALLENGES:

The Information Industry faces a variety of challenges. Among the most critical are:
1. Mergers, Acquisitions, and Consolidations. Many IT companies cannot fund their core business and expansion plans from existing revenues. When technology issues plummeted, capital sources vanished.[15] Investments in Internet companies by venture capital firms fell in the second quarter of 2000 and again in the third quarter, marking the first time since 1996 that such funding has declined for two consecutive quarters. Many have been cutting costs by scaling back on expansion plans and laying off workers.[16]

Despite these streamlining efforts, some 210 Internet companies discontinued operations during 2000.[17] Falling valuations, capital constraints, and greater pressure to achieve and maintain profitability forced dot-coms to revisit their long-term business plans.

2. Antitrust. The advent of globalization complicates applying antitrust law to IT and intellectual property. The Sherman Antitrust Act of 1890 and the Clayton Antitrust Act of 1914 do not sufficiently cover this market. Since 1994, the Department of Justice and the Federal Trade Commission have challenged several mergers in the high technology field based on innovation market theory, a new approach to structural antitrust analysis. The innovation market theory is not traditional antitrust in the sense of price-fixing of existing products or "simple" abuse of monopoly power. It is the use of monopoly power specifically to limit innovation and the development of future products. The combination of these "laws and theories" is of great concern to IT corporations.

3. Internet Taxation Policy and Electronic Commerce. As e-commerce grows, federal, state and local governments stand to lose huge amounts of revenue normally collected as taxes on traditional transactions. Proponents of taxation suggest that those who would exempt "virtual storefronts" from sales and the use of taxes are creating an uneven playing field. Opponents of taxation suggest that existing laws need to be clear and that taxation of remote sales may be discriminatory and ultimately impede economic growth and productivity. The outcome will significantly impact companies developing Internet-based capabilities as well as those that depend on those capabilities for business.

4. Electronic Money (e-money). While electronic transactions are on the rise and technological solutions are eliminating some of the barriers that impeded the use of electronic money and other electronic transactions, privacy, monetary policy and security issues still loom on the horizon. Rigid, highly prescriptive rules or regulations to govern e-money are inappropriate and potentially harmful. (See separate essay under ISSUES.)

5. Export Controls and Licensing. US export control and licensing procedures hinder US firms engaged in trade of IT products and services.[18] With the rapid technology turnover characterizing IT products, administering the procedures often takes up to half of a product's lifetime, making it less competitive. The US satellite industry claims State Dept. export rules cost it $1.2 billion in business and more than 1,000 jobs in 2000.[19]

6. Skilled Information Workforce. The IT revolution has created a huge shortage of highly skilled IT workers in the US. The shortage of adequately trained IT professionals impacts government and other parts of the public sector as well as the private sector. (See separate essay under ISSUES.)

7. Critical Infrastructure Protection. The US has quickly become dependent upon computer networks for many essential services, making it vulnerable to Information Warfare attacks. Computer controls, operating over vast information systems networks, direct water, electricity, gas, communications, and other critical infrastructures. A criminal cartel, terrorist group, or hostile nation may seek to inflict economic damage, disruption, death, and degradation of our defense response by attacking the networks controlling those critical infrastructures. (See separate essay under ISSUES.)

8. Public Key Infrastructure (PKI). Interoperability continues to be the greatest challenge for global implementation of PKI. PKI vendors, realizing the enormous commercial potential and the need to move along quickly in product development, recently formed the PKI Forum. In addition, interoperability for joint military operators will be a

challenge since it is projected that we will increasingly be involved in a full spectrum of military operations other than war around the world. (See separate essay under ISSUES.)
9. Bandwidth. As the number of Internet users increases, so does the demand for the rapid deployment of information and telecommunication technologies. The key technical challenge for the continued growth of the information highway is bandwidth. The current Internet transmission infrastructure and available bandwidth capacity cannot keep up with the higher demand. (See separate essay under ISSUES.)

OUTLOOK:

Despite the recent instability in the economy, the Information Industry will continue to grow. Sustained demand will continue to foster growth. Whether this growth will match the double-digit levels of the last ten years will depend more on consumer confidence in the overall economy rather than on innovation in the industry. Government demand for IT is insignificant as compared to commercial and consumer demand, making it difficult for the government to influence the industry. Regardless, the commercially fueled growth robustly supports most national security resource requirements. The IT breakthroughs that have increased productivity in new economy businesses will increasingly have the same effect on national security processes. The growing industry will also provide the strategic reserve needed to support surge and mobilization requirements as needed. National security clearly is benefiting from commercial investment but this is also a double-edged sword: without direct government intervention, national security requirements will have little, if any influence on the industry. National security will have little choice but to adapt commercial solutions or pay an increasingly stiffer premium to develop and support unique requirements.

For the near term, the Information Industry will continue to face many challenges. Dot-com failures, Internet service provider (ISP) consolidations, competitive local exchange carrier woes, and intellectual property lawsuits are problematic for the Internet. Thus, government regulation becomes one of the Internet's thorniest issues—some believe the Internet is a public trust that needs governmental protection, while others support a hands-off policy from Capitol Hill. The industry will have to deal with the status of the moratorium on Internet taxation, the slowdown in mergers and acquisitions due to stock devaluations, the effect of the ruling in the Microsoft antitrust lawsuit, how the new administration will balance trade and security issues, and rulings related to intellectual property rights on the Internet.
1. Internet Taxation. In October 1998, Congress passed the Internet Tax Freedom Act (ITFA) in response to mounting tensions regarding Internet taxation. ITFA included a three-year moratorium on multiple and discriminatory Internet taxes and established an advisory committee on e-commerce to identify key issues on taxation policy. In April 2000, the advisory committee submitted its final report. In February 2001, House Policy Chairman Representative Christopher Cox (R-CA) and Senator Ron Wyden (D-OR) introduced the Internet Anti-Discrimination Act. If enacted, the proposed legislation will extend the moratorium five more years and permanently ban Internet access taxes. The House and Senate are expected to pass the bill. (See separate essay under ISSUES.)
2. Mergers, Acquisitions, and Consolidations. According to WebMergers.com, the number of merger and acquisition deals rose from 137 in 1998, to 465 in 1999, and to

910 in 2000.[20] In Standard and Poor's view, this period of consolidation will probably turn out to be a long-term positive. Given their expectations for the economy to stage a comeback in the second half of 2001, they expect the Internet sector to regain some of its past luster. They doubt, however, that these stocks will shine as brightly as they did only a few years ago, because investors, like surviving Internet companies, will also be wiser.[21]

3. Antitrust. There is no consensus in Industry on the preferred judicial remedy in the Microsoft case. Should the remedy be structural (i.e., actual division of the corporation) or behavioral (i.e., fines, suspension, etc.)? Though some competitors relish the thought of the behemoth's "demise," most fear the precedence of a structural remedy via government intervention. The outcome will set the tone within the industry for future business strategy.

4. New Administration—Balancing Trade and Security.

In President George W. Bush's report to Congress on the 2000 Trade Agreements Program and 2001 Trade Agenda, new US Trade Representative, Robert Zoellnick, stressed a continued emphasis on "liberalizing" global markets.[22] This initial portrayal of a "trade-friendly" administration has been tempered by hawkish rhetoric over permanent normal trade relations with China due to the April 1 incident with a US Navy P-3 aircraft. The administration's actions in resolving this incident will indicate what priority trade will have in national security. China represents potentially the second largest IT market next to the US. Should the administration pursue a harsh policy toward China and reduce or cut trade, other nations stand ready to fill China's demand for IT products and services. The US position as world leader in IT trade could be in jeopardy.

5. Intellectual Property Rights. The Internet challenges many old assumptions about the location or jurisdiction of transactions and intellectual property. This has caused government and lawmakers to look to Internet companies to enforce laws that their jurisdiction might otherwise not be able to reach. If there should be a fundamental principle for Internet public policy, it is to draw upon the wisdom of the Hippocratic oath: "first do no harm." There is a natural temptation with technology policy to tinker at the margins to reach desired ends. However, the Internet is evolving with such speed and dynamism that even the best-intentioned interventions can have unanticipated negative consequences. Internet intellectual property rights court cases, such as the issues raised with *Napster*, are spawning legislative activity at every level of government. Without clear impact assessment and suggested ways forward, the future of the digital economy may rest with policymakers rather than innovators and entrepreneurs who made the digital economy possible.

For the long term, the Industry will have to deal with the increasing scarcity of bandwidth, the shortage of personnel in the IT workforce, the improved e-commerce environment enabled by proliferation of PKI, new legislation dealing with on-line privacy, and an increasing partnership with government to deal with the continuing threat to critical infrastructures.

1. Bandwidth. Wireless and wire-line companies will continue to thrive, driving the demand for bandwidth. The issue of the "last mile," the final connection between consumers and the networks comprising the Internet, will be resolved to provide the additional bandwidth for residential and business use. This has a potential to create additional challenges and will stimulate service providers to create new high bandwidth

services and place a higher demand on the network backbone. Use of wireless will provide additional challenges for frequency management. Wireless use is projected to soar from approximately one million users in 2000 to roughly 86.6 million in 2005. From a global perspective, wireless technology will quickly overtake "wired" in those countries lacking this infrastructure. This unimaginable growth poses unprecedented challenges for industry to manage frequency allocation and strategic placement of relay towers throughout the urban and rural landscape. The amount of capital investment necessary to make this technology possible is a multi-billion dollar gamble for telecommunication companies. In the end, only a few of the original players may survive the kamikaze market that keeps driving the cost of communications down.

2. Shortage of personnel in the IT Work Force. The inadequate supply of highly trained IT professionals has placed a strain on US technology industries. The industry faces a loss in market share in the global economy due to an inadequate supply of domestic personnel in the technology workforce. Technology work visas, H-1Bs, for foreign workers make up 45 percent of visas issued. The industry rallied Congress to issue an additional 50,000 visas to bring the number to 195,000 in 1999. The adoption of IT curriculum in K-12 and colleges as well as on-the-job IT training will help curtail the critical domestic IT personnel shortage hampering industry today.

3. E-commerce. With the dot-com debacle and the movement by some large firms like Disney Corporation away from on-line services, some have interpreted e-commerce as reaching its peak. But e-commerce is more than setting up a web page. It has evolved from consumers conducting basic transactions on the web to a complete redesign of how business partners, suppliers, and customers interface. Businesses will have to respond quickly to sudden changes in market—the business with the most flexibility and the quickest response time will be the one that succeeds. IT-enabled e-commerce will provide the built-in flexibility features such as content management, order management, dynamic pricing and payment, and international trading capabilities required for success.

4. Critical Infrastructure Protection. CIP is a shared responsibility. The current efforts are yielding incremental results as government and industry sector leaders have begun to share information through Information Sharing and Analysis Centers and the Infraguard Network, established and maintained by the National Infrastructure Protection Center. We will never be able to eliminate every vulnerability within our critical infrastructures, but with continuing cooperation, government and industry can manage the risk to an acceptable level.

GOVERNMENT GOALS AND ROLES:

IT is essential to the future of US economic prosperity and national power. The federal government faces a broad spectrum of issues and challenges. The top four issues where government plays a potentially increasing role are the need for a federal chief information officer, critical infrastructure protection, educating an IT workforce, and taxation of e-commerce.

1. Federal Chief Information Officer (CIO). The time has come for the federal government to realize that technology is critical to the delivery of its services—IT can no longer be considered overhead, but rather be treated as a capital investment. Considering the federal government spends upwards of $40 billion each year on IT, many senior

government officials say it is time to put someone clearly in charge. A federal CIO must be a central managing figure for all IT organizations, reporting directly to the president, controlling a budget independent of the individual agencies, and having the authority to initiate and execute cross-agency IT programs for consistency and elimination of duplication. The CIO should be knowledgeable enough to tackle technical issues relating to security and privacy, skilled in handling management problems such as IT skill shortages, wise in solving social quandaries, and politically astute to satisfy Congress and the President. A possible recommendation for a federal CIO would be someone who currently resides in government who has the reputation and ability to provide the vision, communication, coordination, and innovation necessary to maximize government effectiveness in using IT. In addition, we should ensure enforce Clinger-Cohen, the law governing IT management.

2. Critical Infrastructure Protection (CIP). Government's basic approach to CIP is built around policy preference rather than regulatory actions. In an economy as complex as the US, cooperation with private industry offers the best means to achieve our shared goals in this emerging area. One of the key elements of this cooperative approach is to establish information sharing measures and work with the private sector as well as local and state governments to mitigate infrastructure vulnerabilities at these levels. We strongly recommend that Presidential Decision Directive 63 (PDD-63) be elevated to an executive order. Government Agencies and private sector leaders must continue to concentrate on the milestones already identified by the PDD-63 efforts. They must constantly review vulnerability assessment efforts, develop education programs, and communicate feedback on the status of the National Critical Infrastructure Plan.

3. IT Workforce and Education. Government must partner with industry and academia to resolve the shortage in the IT workforce. In the long term, the government must address increasing the supply of IT professionals from US academic and vocational institutions. The government must act as an advocate for IT career development programs, providing access to information technology in the classroom to motivate future generations of IT professionals. It must provide scholarship programs and tax incentives to foster continued participation in these IT development programs. It should include incentives for minority, women, and disabled workers. In addition to building up the supply, the government must also focus on hiring and retaining its own corps of IT professionals. It should work to streamline hiring processes and provide cross training programs to assimilate new IT employees. It must continue to offer bonuses and higher salaries to retain federal IT workers. (See separate essay under ISSUES.)

4. Internet Taxation on e-Commerce. As part of IFTA, Congress established an advisory committee on e-commerce to identify key issues impacting taxation policy. The committee recommended extension of the moratorium until 2006. This issue is at a critical and fragile juncture of this country's economic expansion and this moratorium will provide some measure of stability for the business community. Extension would indicate that government vigorously supports continued expansion of the industry.

5. Export Control and Licensing. The government must work with US firms to balance economic aspects of national security, i.e., competitiveness of US firms, with the military aspects of national security as it attempts to limit the proliferation of technologies applicable to military purposes. In many cases, "the genie is out of the bottle" and the US approach must switch from controlling proliferation to planning for proliferation.

The government must recognize the advantages in proliferating US technologies over foreign competitors in those areas where proliferation has become uncontrollable. Only then will the US maintain the lead in the IT market.

ESSAYS ON MAJOR ISSUES

ISSUE: THE INFORMATION TECHNOLOGY WORKFORCE

Information Technology (IT) has drastically reshaped the American economy. In recent years, our economy grew considerably because of IT (a whopping 35% in 1989). However, the IT revolution has created a shortage of highly skilled IT workers in the United States. In a recent study conducted by The Information Technology Association of America (ITAA), the number of unfilled IT positions at U.S. companies is projected to be approximately 400,000 over the next 12 months and mushrooming to 1.3 million by 2003. The security of the Department of Defense's information infrastructure is at great risk due to the shortage of adequately trained IT professionals, particularly in the area of information assurance. The shortage of IT workers is also critical in other parts of the public sector as well as the private sector. The shortage is estimated to be costing Silicon Valley companies alone $3 billion to $4 billion a year in lost production. The shortage has the potential of staggering the US's economy and its position as a global technology leader. Dr. Neal Lane, former president of the White House Office of Science and Technology Policy, stated: "I see this as the greatest challenge we have as a nation."

There are several possible alternatives to solving the problem of hiring and retaining skilled IT workers as shown below:

1. Foreign Immigrants: Last year Congress approved legislation to help US companies fill a national shortage of IT workers. The bill allows the Immigration and Naturalization Service to increase the number of H-lB visas from 115,000 to 195,000 annually for the next six years.
2. Minorities, Women, Disabled and Older Workers: Employers are now looking at underrepresented groups in order to fill IT shortages. The Council on Competitiveness is one of the forces behind acquiring more women, minorities, and people with disabilities into high-tech fields.
3. Education: In the Information Age, the focus is on how one uses knowledge and skills to solve complex problems. Students must be able to demonstrate that they are capable of, rather than ingesting information and performing well in examinations. They must be able to draw on their whole range of experience and apply what they know in creative ways. In order for students to be prepared to meet the challenges and expectations of the information-age, they must be technologically literate. Research demonstrates that early preschool years are critical for skill formation. Education programs that intervene early in life have proven to be more cost effective than later remediation attempts. Science and mathematics are the foundation for technical skills, and development of these skills begin in the student's early years. IT companies believe that American colleges and universities are not producing enough students with sufficient knowledge and skills in IT. The Department of Commerce recommends greater interaction between IT companies and schools on all levels, so that the schools can quickly reflect the changing skill sets within their curriculum. Thus, we must focus on knowledge, creativity and the ability to analyze and solve complex situations. The adoption of this methodology in the education curriculum would ensure employability of students in the 21st Century and curtail the critical IT personnel shortage hampering industry today. The U.S. cannot hope to sustain competitive advantage without the assurance that every able-bodied person can effectively participate in growth of the economy. K-12 education is a means to this end.

4. Recruitment Bonuses and Higher Salaries: The single biggest challenge facing the Government relative to obtaining and retaining skilled IT workers is the budget. However, the Office of Personnel Management (OPM) took a major step forward last November when they established higher pay rates for IT workers (computer specialists, computer engineers, and computer scientists) in grades GS-5 through GS-12. Those affected got pay increases of 7% to 33% along with training and education programs, comprehensive benefits and insurance packages.
5. Streamlining the Government Hiring Process: OPM is working to streamline the complicated government hiring process by using Web-based tools. They will add a search option for IT occupations within government to make it easier for tech workers to find job openings.
6. Partnerships: Big industry employers are teaming up in an effort to solve the IT shortage problem by pairing employees' skills with available jobs across the US. ITAA sponsors an annual convention whereby hundreds of key practitioners in education, government and the IT industry come together to discuss technology skill development for workers as well as diversity and image of the high tech worker.
7. Outsourcing: Because of the shortage, public agencies are increasingly relying on contractors for computer work. Given the new awareness of asymmetric threats, the current trend towards outsourcing IT functions raises concerns regarding using non-federal workforce to perform functions that are key to our success on the battlefield.

Recommendation:

To maintain its global economic leadership, the US must invest in the IT workforce and ensure employers can find "the right person with the right skills at the right time." Industry, professional organizations, academia and government need to recognize and support the trend toward lifelong learning. There needs to be continued partnerships with industry, academia, and civic organizations and regional symposia to highlight and develop successful community-based solutions. The Government needs to be a stake-holder with a shared responsibility in problem resolution by establishing commissions focusing national attention on this critical issue and conducting targeted, results-oriented research like the 21st Century Workforce Commission and the Commission on the Advancement of Women and Minorities in Science, Engineering and Technology Development. It will take a concerted effort on everyone's part and implementation of all of the possible alternatives identified, to meet this challenge head-on!

Jackie Lietzel, Laura Shoaf, and Theresa Jackson

ISSUE: BANDWIDTH

The last ten years have witnessed an incredible revolution in the information and telecommunication industry. Powered by the Internet, the information revolution of the 1990's has profoundly changed the lives of the people around the world. As the number of Internet users increases, industry must deploy information and telecommunication technologies more rapidly than ever before.

Perhaps the key technical challenge for the continued growth of the information highway is the speed bump called "bandwidth." The latest Internet applications such as multimedia, phone-quality speech, real time audio and video, as well as mobile Internet all require timely transfer of information and high bandwidth capabilities. With society becoming more mobile and dependent on data transmitted over the Internet, the demand

for wireless Internet services is similarly growing. Wireless devices, including hand-held computers, wireless modems, cell phones and two-way pagers, will eventually displace the personal computer as the preferred Internet access device. The current Internet transmission infrastructure and available bandwidth cannot keep up with the demand.

There are several key wire and wireless technologies now available, with others in development, that will provide much higher bandwidth capacity. These technologies include Cable Television, Internet Service Digital Network, Direct Subscriber Links, T-1 lines, and satellite. These technologies use a variety of mediums (e.g., coaxial cable, fiber optics, microwave antennae, and satellite communications) to provide greater bandwidth capability for telecommunications and Internet application operations. Each technology has its benefits and challenges. The IT Industry is working on near-term solutions to these challenges, to include Internet protocols for gigabit networks, compression mechanisms, and forward error correction coding.

Industry is also increasingly pressuring the US government for the reallocation of federally owned spectrum. The high bandwidth demands for new wire and wireless technologies face greater difficulty in finding available frequency bands—especially any with little or no impact to defense and other federal systems. The need for finding technical solutions to this competition for spectrum is becoming very important. A promising technology to fill this need is laser communications.

Recommendation:

There are areas where the US Government should be more involved because of its dependence on IT. Since the government is a small IT customer compared to the commercial world, it no longer has the muscle power of the past. Thus, it should work closely with industry to leverage the efforts of the latter in this area. The government should also fund the development of IT unique to its requirements and partner for long-term research and development projects in dual use technologies, such as laser communications. Finally, the government should balance its desire to foster economic growth with that of providing an adequate, reliable national defense. These two national goals may come into conflict when dealing with reallocation of federally owned frequency bands. The government may soon be required to make some tough decisions. It must not make them in isolation, but only after serious consideration of all parties' interests and all the elements of national power.

Ivette Falto-Heck

ISSUE: CRITICAL INFRASTRUCTURE PROTECTION (CIP)

America has quickly become dependent upon computer networks for many essential services, making it vulnerable to Information Warfare (IW) attacks. Operating over vast information systems networks, computers control water, electricity, gas, communications, transportation, and other critical functions. In a future crisis, a criminal cartel, terrorist group, or hostile nation will seek to inflict economic damage, disruption, death, and degradation of our defense response by attacking those critical networks. IW has no front line. Potential battlefields are anywhere networked systems allow access. The vulnerability of these systems is poorly understood and the means of deterrence and retaliation are uncertain. In sum, the US homeland may no longer provide a sanctuary from outside attack. For the US to assure the continuity and viability of its critical

infrastructures, these vulnerabilities will require flexible, evolutionary approaches that span both the public and private sectors, and protect domestic and international security.[23]

The government is very active in CIP. Much of its effort came in preparation for the possibility of disastrous events related to the anticipated problems of the year 2000 (Y2K) issue. Recognition of our dependence on IT systems embedded within our daily lives resulted in high level direction focused on identifying what the nation must view as critical infrastructure. Industry and government agencies are working together to identify plans of action and associated milestones should an accidental or intentional event disrupt that infrastructure. The vehicle that directs this effort is Presidential Decision Directive 63 (PDD-63). PDD-63 identified and categorized eight segments of our national industrial capability that must be protected at all costs:

- Information and communication
- Banking and finance
- Water supply
- Aviation, highway, mass transit, pipelines, rail and waterborne commerce
- Emergency and fire services, continuance of government
- Electrical power, oil and gas production and storage
- Public health services
- Research and development

The nation has relaxed with the passing of the Y2K "crisis." Most Americans do not understand the significance of the potential disruption of our critical infrastructures. The US government must initiate a public campaign aimed at educating our society—not to scare the populace but reassure them there are plans in place to secure the infrastructure, minimize the impact, and quickly correct any failure of that infrastructure.

Recommendations:

Government's basic approach to CIP is built around policy preference rather than regulatory actions. In an economy as complex as ours, cooperation with private industry offers the best way to achieve our shared goals in this emerging area. One of the key elements of this cooperative approach is to establish information sharing measures and work with the private sector as well as local and state governments to mitigate infrastructure vulnerabilities at these levels. We strongly recommend that PDD-63 be elevated to an executive order. Government Agencies and private sector leaders must continue to concentrate on the milestones already identified by the PDD-63 efforts. Government and industry must constantly review vulnerability assessment efforts, develop education programs, and communicate feedback on the status of the National Critical Infrastructure Plan.

1. The US Government should establish an Executive Agent[24] that is responsible for helping to protect the nation's Critical Infrastructure from IW.
2. The next version of the National Plan for Information System Protection needs to engage industry, private and public efforts, state and local governments, and incorporate international issues.
3. Since state and local governments make up most of the emergency services first responders and perform the critical coordinating function in local areas, they are at in a better position to deal with industry infrastructures that serve community. Additionally, state and local laws / policies can effectively and efficiently influence the infrastructure industry within their jurisdictions.

4. Government and private industry need to identify issues of interdependencies between sectors. This effort needs to define a real-world business case for sector's dependencies, and identify a business case for developing a common risk assessment approach across sectors.
5. Some major legislative and regulatory challenges must be resolved before we as a nation can make substantial progress. These challenges include: Freedom of Information Act, antitrust, liability, and updating the laws to apply to cyber crimes both nationally and internationally.
6. Our success depends on the awareness within industry and government. There is a need for awareness activities to serve as a repository of outreach efforts, to develop effectiveness metrics for key audiences, and to identify gaps that need to be addressed.
7. There is substantial research and development effort within the federal government and industry related to CIP. However, there needs to be a process to recommend to industry where to focus its efforts and to help government avoid duplication.
8. Much of the industry operates internationally. Therefore, this effort needs to address prevention, response, and cooperation on a global scale. We need to actively engage in international outreach, to encourage countries and international unions, such as the European Union, to develop similar partnerships, and to share information regarding threats, vulnerabilities, countermeasures, and best practices.

Iftikhar Jamil and Floyd Hehe

ISSUE: ELECTRONIC MONEY

Rumors are floating that "cash" is on its way out and "electronic money" (e-money) will replace it as a form of currency. Cash is expensive, inequitable and unclean. Yet, billions of dollars are drained from the economy annually to pay for the printing and care of the US currency. An alternative for cash is electronic money. While technological solutions are eliminating some of the barriers that previously impeded the use of electronic money, privacy, monetary policy and security issues still loon on the horizon.

Electronic money is networked money, money on a card, on a computer, clean – perfect money. Its an old concept that is experiencing new uses provided through advances in computer networks, in processor speed, databases, and the desire of businesses to have remote access and more convenient financial transactions. Some products in the market for consumer use include smart cards, stored value cards, "cybergold" and "beenz". However, without clear and expressed disclosure agreements and stringent security measures for protection of privacy, e-money will not replace cash. What we will see is an increase in uses for e-money.

E-money is currently in an early stage of development. It's difficult to develop policy that is both timely and appropriate without stifling innovation. For this reason, rigid and highly prescriptive regulations and rules are inappropriate and potentially harmful.[25] Near term recommendations include businesses implementing self-regulation and government monitoring of electronic payments on a case-by-case basis.[26] Over the long term, self-regulating may not fully address all issues and may require government intervention to ensure the safety and soundness of electronic payment systems and to protect consumers.

Privacy rights of individuals must also be considered and balanced with the benefits associated with electronic commerce and the free flow of information. Consumer's

privacy must be protected for financial and personal information stored in electronic records, stored-value devices or personal data generated in connection with the financial transactions performed using any method of electronic commerce. Providers of e-money should not collect, trade or sell information about a consumer's transactions without the express written permission of the consumer to the activity.

While substantial improvement have been made in computer security, risks to e-money systems can occur in the consumer or merchant domains as well as network security. There is no single security measure that is sufficient for a particular product. Security risk mitigation efforts include cryptography and monitoring the systems on an on-going basis for attempted breaches.

The end of cash is not here yet! It will continue to be the main currency for the near future as we witness an increase in the use of electronic money. Money is about confidence and there is a strong need for resolution of financial privacy, monetary policy and security issues associated with e-money before it will become the main currency.

Recommendations:

1. Policy: Allow businesses to continue self-regulation and government monitoring of electronic payments on a case-by-case basis. If self-regulating does not fully address all issues over the long term, government intervention to ensure the safety and soundness of electronic payment systems and protection of consumers should be considered.
2. Privacy: Full disclosure by data gatherers should be mandatory. Disclosure will empower consumers to obtain knowledge about why information is being collected and enable better decision-making regarding whether or not they will participate.
3. Security: Strong security risk mitigation efforts are required. Trustworthy cryptography and national standards must be developed and disseminated, privacy preserved and liability conditions established under government coordination.

E. Rowe Campbell

ISSUE: PUBLIC KEY INFRASTRUCTURE (PKI)

PKI is the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates and provides the critically needed support to applications providing confidentiality and authentication of network transactions as well as data integrity and non-repudiation. PKI includes Certificate Management and Registration functions. PKI provides a high degree of confidence that: private keys are kept secure; specific public keys are truly linked to specific private keys; and the parties holding public/private key pairs are who they claim to be.

Public Key Cryptography. Conventional cryptography uses a single mathematical "key" for both encryption and decryption of data. This type of cryptography is known as symmetric cryptography. Public key cryptography uses two keys. One key is kept private, and the other key is made public. The public key is used to encrypt a message, and the corresponding private key is used to decrypt the message.

Digital Signature. Public key cryptography makes digital signatures possible. These signatures can be used to verify the origin of a message. To sign a message indicates that a mathematical algorithm is used to produce a special summary of that message. This summary is then encrypted using the sender's private key. The result, referred to as a digital signature, is then appended to the message. The addressee can confirm both the origin of the message, and the integrity of the information therein, by decrypting the

digital signature using the originator's public key and comparing the result with a summary produced by passing the received message through the same mathematical algorithm. The process sounds complicated, however, it can as simple as selecting an icon on a computer screen.

Link to e-Commerce. A PKI is a critical element of national e-commerce; it ensures the security of electronic transactions, and the exchange of sensitive information between parties that do not have a prior established business relationship. The economic and social benefits of the information highway can never be fully realized without the assurance of a secure infrastructure.

Infrastructure Protection. To enable seamless and trustworthy electronic business transactions, an infrastructure is needed that supports a common set of security services in a standard fashion. This in turn supports wide-scale interoperability, and the realization of the full capabilities of all technologies used in business applications. For example, financial transactions could be digitally signed and verified at the intended destination in a reliable fashion. Secure e-commerce is possible on a global scale once a common set of security infrastructure standards are agreed upon by global partners.

Third-party Trust. Third-party trust is a fundamental requirement for any large-scale implementation of security services based on public key cryptography. Third-party trust implies that two individuals implicitly trust each other, even though they have not previously established a business or personal relationship. Public key cryptography requires access to a user's public key. In a large-scale network, however, it is impractical and unrealistic to expect that each user will have previously established relationships with all other users. In addition, because a user's public key needs to be widely available, the association between a public key and a specific individual must be guaranteed by a trusted third party, in order to prevent impersonation of legitimate users. A trusted third party, operated in a secure manner, allows users to implicitly trust any public key certified by that third party. A third-party certification agent is referred to as a "Certification Authority" (CA).

Certification Authority (CA). A CA is a trusted individual whose primary responsibility is certifying the authenticity of users. In essence, the function of a CA is analogous to that of the passport-issuing office in a government. A passport is a citizen's secure document, issued by an appropriate authority that certifies that the citizen is who he/she claims to be. It is effectively that person's "paper identity". Any country trusting the authority of the first country's government passport office will trust the citizen's passport.

Certificates. A network user's certificate is the electronic equivalent of his/her passport. It contains information that can be used to verify the identity of the owner. A critical piece of information contained in a user's certificate is that owner's public key. A public key may be used either to encrypt data destined for the certificate owner, or to verify the owner's digital signature.

Department of Defense Implementation of PKI. DoD is implementing smart card technology as a Department-wide Common Access Card (CAC). The CAC will be the standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC will also be the principal card used to enable physical access to buildings and controlled spaces and for logical access to the Department’s computer networks and systems. By September 2002, approximately four million cards will be issued worldwide.

Department of Defense Policy for use of PKI. On May 6, 1999, the Deputy Secretary of Defense issued a memorandum that encouraged widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. The strategy to achieve the target DoD PKI is a key element of the overall DoD strategy for achieving information assurance. On November 10, 1999, the Deputy Secretary of Defense directed that the CAC be used as the DoD's primary platform for the PKI authentication token. Section 374 of the fiscal year 2000 Defense Authorization Act (Public Law 106-65) required the evaluation of the option of using the smart card as the DoD's authentication token. DoD responded in a report to Congress, "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier," January 10, 2000. The report concludes the smart card is the most feasible, cost-effective technology for the authentication mechanism to support the DoD PKI and to protect its critical information. However, implementing new technology like the CAC DoD-wide has a number of risks associated with it. An initial concern would be technology refresher. Do we have the hardware, software and trained personnel in place to maintain 4 million smart cards? It may cost more to maintain the CAC than it did to purchase it. This may be the perfect case where industry is better prepared to manage a technology that will benefit all.

A main driver of PKI technology is the world's growing dependence on the Internet. PKI will play a large role in securing all types of e-business activities. When properly implemented, Public-key cryptography offers significant security benefits. Web-based applications, e-commerce, mobile users, financial institutions and companies whose public role exposes them to every form of digital criminality are seeking guaranteed levels of security. Many seem to think implementing a PKI will give them the edge they are looking for.

Ray Montford

ISSUE: ON-LINE PRIVACY

In May 2000, the Federal Trade Commission (FTC) released a report in which a narrow majority of commissioners recommended "Congress enact legislation that, in conjunction with self-regulatory programs, will ensure adequate protection of consumer privacy online." Most in the IT industry and two of the five FTC commissioners, vehemently oppose the FTC's position. A classic battle is unfolding to find a delicate balance between individual rights, industry growth, and government intervention.

On-line privacy revolves around the protection of personal information collected by commercial entities over the Internet. Consumer concerns about their online privacy may inhibit the strong potential growth in our economy promised by the Internet. Industry opposes strong government intervention to address these worries, as a direct threat to the expansion of e-commerce. Either way the issue has the potential to inhibit a major potential expansion of our national economy.

Four areas offer alternative solutions to the problem:

1. Industry Self-Regulation. Many companies are taking strong steps to protect consumer privacy because they feel it makes good business sense to do so. This is the preferred approach by all groups including the use of "seal" programs, industry groups, and Corporate Privacy Officers. However, some believe the industry reaction has been slow and that there is a weak business motivation to protect consumer privacy.

2. Consumer Empowerment. To support these consumer preferences, technologies are emerging which might help solve the problem. This approach allows consumers to implement their individual preferences with some potential performance impact.
3. Education. Proponents of this approach believe that consumer education efforts can bring market demand forces to bear. In addition, industry groups are educating their member companies on proper privacy practices. All support efforts in this area.
4. Regulation. Congress can enact legislation that regulates consumer-oriented commercial Web Sites. Generally, these regulations focus on four "widely accepted" fair information practices, which address notification of a site's information practices; consumer choice on how their information is used; consumer access to stored information; and steps necessary to protect consumer information. This approach addresses compliance issues. It has political benefits, allowing Congress to show response to constituency concerns. However, it may be premature and unnecessary. There are complex issues to resolve and implementation cost may reduce the competitive advantage of e-commerce.
Recommendations:
1. Avoid comprehensive online privacy legislation and/or regulation. Instead, focus efforts on enforcing and learning from laws passed in higher risk areas such as children's privacy, banking and personal health. Congress should give the FTC the authority to set basic standards for fair information practices which are technology neutral. As a minimum, these basic standards should require businesses to inform consumers what personal information they are collecting and what they are doing with it.
2. Strongly support industry self-regulation efforts as the primary privacy implementation mechanism. Congress should also review existing FTC authority to prosecute privacy abusers and determine if it is adequate to hold companies accountable.
3. Conduct a joint campaign with industry to promote consumer education with special emphasis on how consumers can use tools to make their own privacy choices.

Tony Dominice

ISSUE: INTERNET TAXATION

The "tax debate" is as old as civilization itself and even in the 21st century the parties to the debate can find neither peace nor peaceful co-existence, but rather a mutual distrust and disdain. Proponents of taxation suggest that an uneven playing field is being created by those who would exempt "virtual storefronts" from sales and use taxes. Opponents of taxation suggest that existing laws should be streamlined and clarified and that taxation of remote sales may be discriminatory and ultimately impede this nation's economic growth and productivity sparked by the digital economy.

One has to but examine the economic impact of the IT sector, to include the Internet, as well as the skyrocketing growth of electronic commerce to appreciate why so many in government see the opportunity for revenue generation. The Information Industry has spawned unparalleled economic growth in the form of productivity gains, innovation that facilitates greater efficiencies and shorter production cycles and "frees up" capital permitting reinvestment. The Department of Commerce has reported that while production by the IT sector accounts for only 8 percent of the Gross Domestic Product (GDP), its rapid 18.8 percent real growth rate from 1994 to 1998 accounted for 35

percent of the nations real economic growth.[27] By comparison, the average growth of the overall economy during the same period was approximately 4 percent.

In response to the mounting tensions with respect to taxation of the Internet, Congress intervened in October of 1998 via passage of the Internet Tax Freedom Act or IFTA. The primary objectives of IFTA were to provide a three-year moratorium on multiple and discriminatory Internet taxes and to establish an advisory committee on electronic commerce to identify key issues impacting taxation policy.

The Advisory submitted its report to Congress in April 2000 and included the following key provisions:

- Extend the current moratorium on new multiple and discriminatory taxes through 2006.
- Simplify and clarify existing Sales and Use Tax laws (specifically with regard to remote sales tax collection and the "nexus issue" or what constitutes "presence" in a state.
- Encourage state and local governments to work collectively to streamline and simplify sales and use tax policy that protects individual privacy.
- Establish permanent moratorium on Internet access taxes.
- End the 3 percent federal excise tax on telecommunications (first enacted to pay for the Spanish American War of 1898).
- Support the current moratorium on tariffs and duties for electronic transmissions established by the World Trade Organization and continue to monitor international activity in this arena.

There are three possible policy options with respect to the appropriate role of government regarding the taxation of remote sales:

1. Government should withdraw immediately from the Internet tax debate and permit the free market to drive the behavior of the economic actors to include businesses, consumers and state executives. Although admittedly, due to its intervention through passage of the IFTA one cannot "un-ring the bell" we can still permit the current moratorium to lapse and allow the market place to be the driving force.
2. Government should extend the current moratorium through 2006 as is currently proposed permitting the states time to cooperatively streamline and simplify current law with respect to sales and use taxes and clarify what establishes "nexus" or a business' "presence" in a state. This policy option would also include the appropriation of funds.
3. Government should not extend the moratorium, but support the recommendations of the report submitted by the Advisory Commission in accordance with IFTA by appropriating funds to permit their accomplishment by the states.

Recommendation:

Of the three options, we recommend option #2, extension of the moratorium through 2006. We are at a critical and fragile juncture of this country's economic expansion and the moratorium would provide some measure of stability and signals to the business community that we want them to vigorously pursue expansion. Although the other options could perhaps achieve the same ends, we do not believe it would occur as rapidly or as orderly.

Nancy Myrick

CONCLUSION

Information permeates every aspect of the way we live. The rise of the new economy is directly attributable to the development of information technologies that transform simple data into vast knowledge and insight and that provide the global interconnectivity to share that knowledge and insight nearly instantaneously around the world. The US Information Industry is poised to meet the growing demand for IT products and services. It is a booming, dynamic industry, characterized by merger, acquisition, and consolidation.

The recent turmoil in the economy, induced by the devaluation of technology stocks, resulted in less capital available for growth and has forced many firms in the industry to adjust their business strategies accordingly. However, sustained demand for IT will continue to foster growth. Whether this growth will match the double-digit levels of the last ten years will depend more on consumer confidence in the overall economy than on innovation in the industry. The Information Industry will continue to pace the growth in international trade, despite the transient effects of the current economic slowdown. The US will continue to lead the global IT market even though it may maintain a trade deficit for the near future. Simpler, less restrictive trade controls and licensing procedures will increase exports, alleviating the trade deficit and preserving the US lead.

Government demand is insignificant compared to commercial and consumer demand, making it difficult to influence the industry. Regardless, the commercially fueled growth robustly supports most national security resource requirements. The IT breakthroughs that have increased productivity in new economy businesses will increasingly have the same effect in national security processes. The growing industry will also provide the strategic reserve needed to support surge and mobilization requirements if required. National security clearly is benefiting from commercial investment but this is also a double-edged sword: without direct government intervention, national security requirements will have little, if any influence on the industry. National security will have little choice but to adapt commercial solutions or pay an increasingly stiffer premium to develop and support unique requirements.

BIBLIOGRAPHY

Bensinger, Ari, *Standard & Poor's Industry Surveys, Communications Equipment,* (New York, McGraw Hill Co., January 18, 2001)

Bernkope, Mark, "Electronic Money and Monetary Policy," First Monday, 1996

Graham-Hackett, Megan, *Standard and Poor's Industry Surveys*, (New York, McGraw-Hill Co., September 14, 2000), p.1

Graham-Hackett, Megan, *Standard & Poor's Industry Surveys, Computers: Networking*, (New York, McGraw Hill Co., September 14, 2000)

Graham-Hackett, Megan, *Standard & Poor's Industry Surveys, Computers: Hardware,* (New York, McGraw Hill Co., December 14, 2000)

Kessler, Scott H., *Standard & Poor's Industry Surveys, Computers: Consumer Services & the Internet*, (New York, McGraw Hill Co., March 1, 2001), p.1-13.

President's 2000 Annual Report to Congress on the Trade Agreements Program and 2001 Agenda, Office of the US Trade Representative, Press Release, March 7, 2001 (Annex I, US Trade in 2000, report available at http://www.ustr.gov/reports/2001.html)

"Retail E-Commerce Sales for The Fourth Quarter 1999 Reach $5.3 Billion," Press Release, US Department of Commerce, Census Bureau Reports (rel. Mar. 2, 2000).

Rudy, Jonathan and Jim Corridore, *Standard & Poor's Industry Surveys, Computers: Commercial Services,* (New York, McGraw Hill Co., January 25, 2001)

Rudy, Jonathan, *Standard & Poor's Industry Surveys, Computers: Software,* (New York, McGraw Hill Co., October 5, 2000)

US Industry & Trade Outlook® 2000, (New York, McGraw Hill Companies, US Department of Commerce/International Trade Association)

US Trade Representative Annual Report 1999, Committee of Participants on the Expansion of Trade in Information Technology Products, Status, March 2000.

The White House, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," WHITE PAPER, May 22, 1998

Wohl, Philip D., *Standard & Poor's Industry Surveys*, *Telecommunications: Wireless*, (New York, McGraw Hill Co., December 28, 2000)

Wohl, Philip D., *Standard & Poor's Industry Surveys*, *Telecommunications: Wireline*, (New York, McGraw Hill Co., September 28, 2000)

[1] Megan Graham-Hackett, *Standard and Poor's Industry Surveys,* (New York, McGraw-Hill Co., September 14, 2000), p.1

[2] Ari Bensinger, *Standard & Poor's Industry Surveys, Communications Equipment,* (New York, McGraw Hill Co., January 18, 2001)

[3] Jonathan Rudy and Jim Corridore, *Standard & Poor's Industry Surveys, Computers: Commercial Services,* (New York, McGraw Hill Co., January 25, 2001)

[4] Scott H. Kessler, *Standard & Poor's Industry Surveys, Computers: Consumer Services & the Internet,* (New York, McGraw Hill Co., March 1, 2001)

[5] Megan Graham-Hackett, *Standard & Poor's Industry Surveys, Computers: Hardware,* (New York, McGraw Hill Co., December 14, 2000)

[6] Megan Graham-Hackett, *Standard & Poor's Industry Surveys, Computers: Networking,* (New York, McGraw Hill Co., September 14, 2000)

[7] Jonathan Rudy, *Standard & Poor's Industry Surveys, Computers: Software,* (New York, McGraw Hill Co., October 5, 2000)

[8] Philip D. Wohl, *Standard & Poor's Industry Surveys, Telecommunications: Wireless,* (New York, McGraw Hill Co., December 28, 2000)

[9] Philip D. Wohl, *Standard & Poor's Industry Surveys, Telecommunications: Wireline,* (New York, McGraw Hill Co., September 28, 2000)

[10]Scott H. Kessler, *Standard & Poor's Industry Surveys, Computers: Consumer Services & the Internet,* (New York, McGraw Hill Co., March 1, 2001), p. 13

[11] *US Industry & Trade Outlook® 2000,* (New York, McGraw Hill Companies, US Department of Commerce/International Trade Association) contains industry and product shipment data, which through 1996 are actual; data for 1997, 1998, and 1999 are estimates, and data for 2000 are forecasts. Data for Total USITO in Table 1 and Figure 1 is the Value of Shipments from Chapters 26, 27, 30, and 31 of the US Industry & Trade Outlook® 2000 and adjusted to constant 1999 Dollars. The chapters in Outlook 2000 were written in September or October 1999. Therefore, we do not believe these forecasts accurately predict the market downturn for the Internet related stocks and corresponding economic downturn of 2000. Standard and Poor's publishes their Industry Surveys semi-annually. Even the latest one at this time (Computers: Consumer Services & the Internet dated March 1, 2001) does not have operating revenues for 2000. Since the S&P data does not include 2000 and the Outlook 2000 forecasts are so old, we did not use 2000 for the table and chart of operating revenues and shipments. When we added the segments together as shown on the total chart, there is amazing correlation between the two sources for the total Information Industry.

[12] Kessler., p. 1

[13] US Trade Representative Annual Report 1999, Committee of Participants on the Expansion of Trade in Information Technology Products, Status, March 2000.

[14] *US Industry & Trade Outlook® 2000,* (New York, McGraw Hill Companies, US Department of Commerce/International Trade Association), Chapters 26, 27, 28, 30, and 31.

[15] TheStreet.com Internet Index, which tracks the performance of a broad range of dot-coms, saw gains of 57% in 1997 (from February when the index was created), 160% in 1998, and 184% in 1999. In 2000, the

index declined by a staggering 74%, under performing all the broad market indicators and just about every other industry segment (Kessler, p. 1)

[16] Following 36% growth in Internet employment during 1999 to 2.5 million workers, about 494 companies laid off 41, 274 people in 2000. (Kessler, p. 3)

[17] Kessler, p. 3

[18] US firms must abide by the procedures established in the Export Administration Regulations. A firm must also abide by the High Performance Computing Act. Finally, due to potential military application of IT products, a firm must also abide by the guidelines established by the Wassenaar Arrangement. Congress tightened down on export controls related to satellite technology because of the loss of nuclear weapons secrets to China. In 1999, commercial satellites and related items were reclassified as munitions, subject to State Department munitions regulations (Wassenaar, etc.). This creates a likelihood that non-military components will at times qualify as munitions.

[19] Frank Mooring Jr., "Space Issues Awaiting White House Focus," *Aviation Week & Space Technology*; New York; March 12, 2001

[20] Kessler, p. 8

[21] *Ibid.*, p. 4

[22] Press Release, Office of the US Trade Representative, President's 2000 Annual Report to Congress on the Trade Agreements Program and 2001 Agenda, March 7, 2001 (Annex I, US Trade in 2000, report available at http://www.ustr.gov/reports/2001.html)

[23] WHITE PAPER, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998

[24] This Executive Agent is different than the current CIP coordinator within the OSTP

[25] "Electronic Money and Monetary Policy", by Mark Bernkope, First Monday, 1996

[26] "Electronic Money and Monetary Policy", by Mark Bernkope, First Monday, 1996

[27] US Department of Commerce, Press Release, "Retail E-Commerce Sales for The Fourth Quarter 1999 Reach $5.3 Billion," Census Bureau Reports (rel. Mar. 2, 2000).