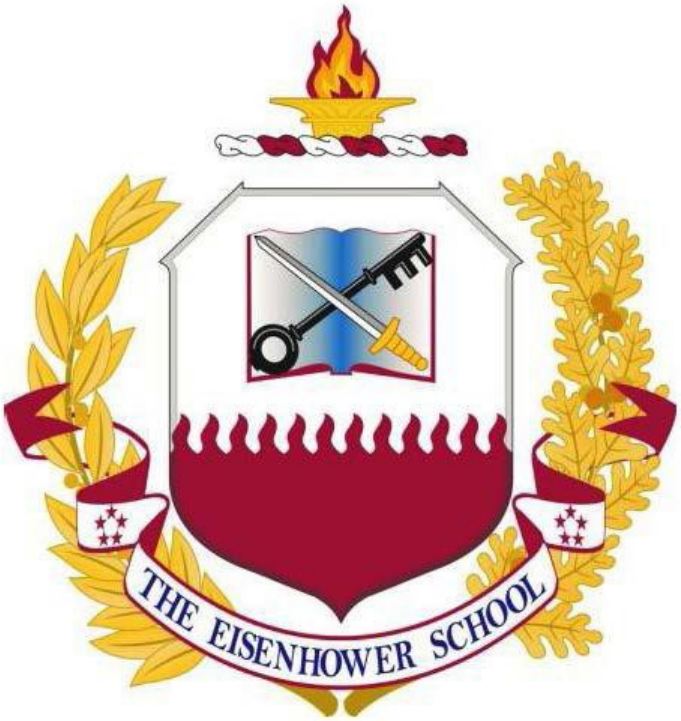
Spring 2016
Industry Study

Final Report
Information and Communications Technology



The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) 2016

ABSTRACT: The ICT industry is diverse, dynamic, and an essential driver of economic growth and national security. The principle challenges for policymakers and private industry are to work together to foster innovation, develop a strong domestic workforce, secure data and ensure privacy, and to implement sensible regulatory policy that helps the industry achieve these objectives. As the world moves toward ubiquitous connectivity and software-defined products and services, the federal government must embrace flexible policies that do not stand in the way of innovation and growth.

COL Abubakar Abu Adamu, Nigerian Army
BG Muhammad Munir Afsar, Pakistan Army
Lt Col Lamont Atkins, US Air Force
Ms. Mindi Bush, Dept of Defense
COL Robert Fago, US Army
LTC Michael Frank, US Army-Army National Guard
Mr. Brian Greaney, Dept of State
LTC Fernando Guadalupe, US Army
CDR Kelly Harrison, US Navy
Lt Col Wade Henning, US Air Force
CDR James Felling Hurt, US Navy
Mr. Bruce Moody, National Geospatial Intelligence Agency
Mr. Edward Paglee, Dept of Homeland Security
Mr. Terry Phillips, Dept of Air Force
Lt Col Esther Sablan, US Air Force-Air National Guard
Ms. Genevieve Sapir, Dept of Transportation

Col Paul Gillespie, PhD, US Air Force, Faculty Lead
COL Richard Altieri, J.D., US Army (Retired), Faculty
Col David King, PhD, Canadian Forces (Retired), Faculty
Mr. Feza Koprucu, Department of Homeland Security, Faculty
Lt Col Todd McAllister, PhD, DSAR Dept, USMC Reserves, Faculty
Col Lynne Thompson, EdD, US Air Force (Retired), Faculty

Industry Study Outreach and Field Studies

On Campus Presenters

Central Intelligence Agency (CIA)
Command, Control, Communications and Computers (C4)/Cyber, Joint Staff J6
Defense Cyber Crime Center (DC3)
FireEye
Government First Responder Network Authority (FirstNet)
Microsoft, U.S. Federal Government Sales
Federal Communications Commission (FCC)
J Capital Research
John Kneuer, President JKC Consulting, Inc.
John Backus, New Atlantic Ventures
U.S. China Economic and Security Review Commission
U.S. Patent and Trademark Office (USPTO)
Verisign

Field Studies—Domestic

AT&T, Washington, DC
Brocade, San Jose, California
Cisco, San Jose, California
Command, Control, Communications and Computers (C4)/Cyber, Joint Staff J6, Washington, DC
CTIA – The Wireless Association, Washington DC
Defense Information Systems Agency (DISA), Fort Meade, MD
Defense Innovation Unit Experimental (DIUx), Mountain View, California
Dell, Plano, TX
Department of Homeland Security, Arlington, VA
Ericsson, Plano, TX
Facebook, Menlo Park, California
Google, Mountain View, California
Huawei, Plano, TX
Hughes Network Systems, Germantown, MD
Information Technology Industry Council (ITIC), Washington DC
International Business Machines (IBM Federal), Washington DC
NASA Ames Research Center, Moffett Field, California
Office of Management and Budget (OMB), Washington DC
OnPoint Technologies, Inc., Silicon Valley, California
Oracle, Redwood City, California
Shape Security, Mountain View, California
Software and Information Industry Association (SIIA), Washington DC
Telecommunications Industry Association, Washington DC
Texas Instruments, Richardson, TX
USCYBERCOM, Fort Meade, MD
Verizon, Ashburn, VA

Field Studies—International

BDA, Beijing, PRC
BYD, Shenzhen, PRC
China Mobile, Beijing, PRC
TCL, Shenzhen, PRC
US Information Technology Office (USITO), Beijing, PRC
ZTE, Shenzhen, PRC

Introduction

For four and a half months, the students of the Eisenhower School's Information and Communications Technology (ICT) seminar studied the ICT industry, combining academic work with direct interaction with firms across the United States and in China. We examined the different markets within the industry, conducted case studies, and leveraged the experience of industry practitioners. We evaluated the industry's role in the domestic and global economy, assessed business strategies for continued growth and innovation, and considered the overall relationship between the industry and the government and its resulting impact on national security.

The industry is widespread, diverse, and embedded in nearly every aspect of American economic, social, and political life. It is also full of contradictions, as competing forces propel us forward and threaten to hold us back at the same time: information technology is simultaneously one of our greatest strengths and threats to national security. While our general assessment is that the industry is strong and resilient, this sector is too diverse and too dynamic for a one-size-fits-all conclusion about the state of the industry.

Among policymakers, industry representatives, and even the authors of this report, there are different ideas on what form the relationship between government and industry should take. But we all agree that now, more than ever, we must take a hard look at the future of this relationship. There will continue to be national security implications for the United States if federal regulations, processes, and acquisition systems cannot become more adaptive and forward-looking. In this paper, we analyze the ICT industry, discuss its challenges and outlook, and offer ideas to promote the two paramount goals of economic growth and national security.

The Industry Defined

The first step in analyzing the dynamic linkage between the ICT industry, innovation, U.S. economic growth, and national security, is to define the parameters of the ICT industry itself. This is no small task: the U.S. ICT industry is diverse, complex, and ubiquitous. It exists everywhere, in terms of hardware and software embedded in almost everything we do, but it also exists nowhere, in that it depends on invisible bits of data that we cannot see or touch.

In this context, the ICT industry is best described as an industry of industries.[1] This study focuses on four principal categories that fall under the ICT umbrella of industries: hardware, software, communications, and services. Those categories are further broken down using recognized ICT markets as defined by the North American Industry Classification System (NAICS) (see the Appendix for a list of the relevant NAICS codes).[2] Within those defined markets, we further narrowed our analysis to focus on certain aspects of the industry with significant potential to affect U.S. national security.

Hardware. The hardware and manufacturing industry includes a wide range of equipment manufacturing and integration markets, including computing devices (laptops, servers, mobile phones) and peripherals, intermediate and enabling technologies like the Global Positioning System (GPS), and network equipment (routers, modems, gateways) that provide the wired and wireless telecommunications capabilities that bind the ICT industry together.

Software and Internet Publishing. The software and Internet publishing industry encompasses the design, production, and support of software required to deliver digital content to users. Markets include software for operating and protecting network equipment and computing devices, as well as software applications for entertainment and productivity. Security software publishing is a notable and fast growing market within this industry due to a rising demand for antivirus, malware/spyware removal, encryption, and firewall solutions. Internet publishing markets include what consumers (both personal and business) actually use such as online content (e.g., news, music, video), advertising, and subscription services.

Communications. The communications industry develops, operates, and sustains wired and wireless network infrastructure for telecommunications. This broad industry includes a diverse array of carriers, providers, and resellers of cable, satellite, telephone, and radio-based cellular connectivity. Internet communications markets include narrowband and broadband access, web hosting, and backbone services (carrier, transit, peer-to-peer and content delivery).

Services. The services industry spans three primary markets: data processing and hosting, consulting, and equipment repair. The data processing and hosting market includes cloud-based computing and related provisioning and management services. ICT consulting includes planning, design, integration, and support services for public and private sectors. Cybersecurity consulting, in tandem with security software publishing, is a particularly fast growing market within this industry.

The Current Condition of the Industry

With an industry as diverse as ICT, broad brush strokes can paint neither an accurate image of the health of the industry nor the net benefit it returns to the nation in terms of economic growth and national security. Each of the four industry categories identified in the previous section have different opportunities and challenges that directly affect performance and viability. The current conditions in these four categories are analyzed below, focusing on the current state of competition, health of major firms, business strategies and vulnerabilities, and foreign market forces.

Hardware. The hardware sector is characterized as mature to declining; revenues across the board are expected to either grow very slowly (<1.5% maximum) or even decline (several subsectors project >2.0% decline over the next five years).[3] Generally, lower overseas labor rates and the resulting inability of the U.S. manufacturers to compete in low-end markets have yielded a transformation of the U.S. market participants into heavy research and development firms that offshore their low-end production and export the high-end products they are still producing in the United States.[4] There is little differentiation between products in the market for personal devices, including personal computers and smart phones, which are produced overseas in low labor rate markets.[5]

While certain companies, such as Apple, have been able to differentiate themselves,[6] customers have significant bargaining power because if one company tries to ask a higher price than their competitors for a product, the customer will either simply wait for the rest of the industry to provide that product at a lower price, or shift to a substitute product. As a result, profit margins

are low across the sector, averaging 4-8%.[7] Competition is intense, and expected to remain so for the next five years.[8] Imports account for large percentages (in all cases, >50% of the markets, some exceeding 90%) of markets in this sector.[9] Employment is also dropping in all markets in this sector, as automation and offshoring are reducing the number of required employees at U.S. firms.[10]

Software and Internet Publishing. Unlike the hardware and manufacturing sector, the software and Internet publishing sector has exhibited healthy growth over the past five years, with revenue growth rates generally higher than 4% and profits around 20%.[11] New market opportunities abound because the shift to mobile computing and cloud computing have lifted the previous storage size restrictions that hindered mobile device software and content development and delivery. The Internet of Things (IoT) is also providing new opportunities across a range of user requirements.[12] The software subsector is not highly concentrated. The three largest firms occupy less than 33% of the total market and there are over 7,000 businesses participating.[13] The Internet publishing subsector, on the other hand, is highly concentrated, with the largest firms, Alphabet (Google's parent organization), Apple, Facebook, Netflix, and Microsoft, occupying greater than 60% of the subsector's market.[14]

The barriers to entry in this sector are moderate, largely because intense competition is offset by low capital intensity and light regulation.[15] Software publishing start-ups can, and frequently do, enter the market with little financial or human capital. Most new startups develop a niche product with an eye toward selling that product (and the entire company) to one of the giants in the sector.[16] Competition both among the giants and among the small companies vying to be acquired by one of those giants is intense.[17] Moreover, there are significant threats to profitability, including software piracy, litigation, an expensive workforce, and high research and development costs. The explosion of private and sensitive data presents special challenges, but also new opportunities for software firms.

Communications. The communications sector has three major subcategories: wireless, wireline, and satellite. The wireless subsector has performed very well over the past five years and is expected to continue to be profitable. Wireless revenue is projected to reach $277.2 billion by 2020 due primarily to growing demand for smart devices as well as the increased number and type of services which can be conducted online.[18] Future profitability, which is expected to be less than in previous years, will depend on the cost and availability of spectrum, the price of semiconductors and other electronic components, and per capita disposable income which is linked to the demand for Internet connected devices.[19]

The wireless sector is the most competitive sector of the industry with a high monthly subscriber churn. Wireless products are increasingly homogeneous, forcing firms to compete primarily on price and only secondarily on service.[20] Despite fierce competition, the threat of new entrants does exist; however, the threat is constrained by the limited supply and high cost of spectrum as well as the high cost of other start-up expenses such as network infrastructure.[21] As a result, four nationwide firms make up approximately 95% of the market with the top two firms together taking 67%.[22] Some firms in other segments of the ICT industry have considered acquiring spectrum via government-sponsored auctions (discussed in more detail in the Selected

Essays portion of this paper), whereas others are seeking to enter the market as re-sellers without acquiring their own infrastructure.[23]

Similar to the wireless sector, the wireline sector is mature and very competitive: the top three firms account for over 60% of market revenue.[24] But while the wireless sector shows strong growth; the wireline sector does not. Market revenue is expected to decline at an annualized rate of 1.4% to $157.9 billion by 2020.[25] As wireless service improves in quality and reliability, consumers are increasingly using wireless services only and canceling landlines to eliminate redundancy.[26] Wireline carriers have tried to keep pace with their competitors by deploying optical fiber networks that provide faster speeds and larger bandwidth capacity than cable or wireless networks.[27] Wireline carriers have also moved to offset the losses from decreased demand of wireline by providing backhaul services.[28] This mitigates some decline, but not all. For example, due to the decreased demand, the workforce in this sector is expected to shrink at an average annual rate of 1.3% to 382,612 workers by 2020.[29] This sector, like the wireless sector, is under significant government regulation, faces high infrastructure costs, and serves customers with high buying power. Although the outlook for this sector is not particularly strong, it nonetheless provides the necessary infrastructure for wireless carriers and satellite operators which are both part of a growing market.

The satellite sector is mature, yet has experienced steady growth over the past five years.[30] Since 2010, this sector has become an important means of providing telecommunications services through the development of the direct-to-home television market, expansion of satellite broadband Internet services, advancement of digital technology, and growth of wireless backhaul services.[31] The sector is moderately competitive with significant barriers to entry and a moderate level of regulation. The industry is comprised of a two-tiered structure with two vastly different types of industry players: larger firms which own and operate satellites, and firms that buy excess capacity from these infrastructure owners and resell the services downstream. The latter firms predominate: nearly 85.0% of satellite firms have fewer than 20 employees.[32]

The satellite sector is expected to continue to grow steadily. Revenue is forecasted to grow 4.3% per year on average to $8.4 billion by 2020.[33] The growth will be driven by increased demand due, in part, to the shortage of spectrum for wireless and the rural telecommunications coverage gap.[34] To compensate for the rural gap, operators are launching high throughput satellites (HTS). HTS increase Internet speeds while reducing prices and correct many of the connection problems that historically plagued the industry, making satellite service competitive both in rural markets and in those where DSL services are present.[35] HTS alone are expected to increase operations at an average annual rate of 1.0% leading to increased hiring (annualized 2.4%) to meet the growing demand.[36] Based on the global nature of satellites, the moderate number of foreign firms in the sector is not surprising. In fact, the fourth largest firm is foreign based.[37]

Services. For the purpose of this paper, computer services encompass both information technology (IT) consulting as well as data processing and hosting services. Although both sectors do provide a service, they behave differently, and therefore are addressed separately in this section. The IT consulting sector has grown in the last five years and will continue to grow at an expected average annual rate of rate of 3.2% to $437.3 billion in 2020.[38] As a labor-intensive sector, there are few barriers to entry in the form of capital investment, but the sector depends on recruiting and

retaining highly skilled workers. The major players have strong brand recognition and tend to market themselves toward other big name clients, leaving much room for small start-ups to enter the market.

Competition is fierce not only within the sector, but also from firms in competing sectors such as management consulting as well as large firms building in-house capabilities.[39] The sector is expected to experience strong growth in the next five years; as U.S. companies reorganize, expand, and engage in mergers and acquisitions, the demand for technology consulting is likely to accelerate. This sector is highly globalized and is likely to become even more so as the global economy becomes more digitized. All U.S. firms in this sector with greater than 2% share of the market also operate overseas and foreign firms are entering the U.S. market as well.[40]

The data processing and hosting services sector has experienced "steady and tremendously strong growth" in the past five years and revenue is expected to continue to grow for the next five years at an annualized rate of 4.2% to $166.2 billion.[41] This growth is a result of companies moving away from internal data management and opting instead to outsource. This trend is likely to continue as the technology required to process and host data becomes more complex and the level of expertise needed to effectively manage large data centers increases. Also, as traditional networking infrastructure is found to be less secure, companies will seek solutions from the third party providers in this sector. The introduction of cloud computing, one of the sector's fastest-growing product offerings, has significantly contributed to the increased demand in this market. This sector is likely to experience a high number of mergers and acquisitions; however, smaller, on-demand freelancers empowered by the growing "gig economy" will continue to service those businesses unable to pay the high costs of the large firms.[42]

Industry Challenges

ICT industry challenges fall into four general categories: cybersecurity, innovation, human capital, and regulatory policy.

Cybersecurity. The seriousness of cybersecurity challenges cannot be overstated. Cyber attacks continue to grow at an alarming rate: more than 317 million new pieces of malware were created last year—nearly one million new threats were released each day.[43] Reports estimate that cyber attacks cost U.S. businesses between $400 and $500 billion a year.[44] But there are not just financial losses. Government information is routinely stolen. Sensitive and personally identifiable information on 21.5 million people has been stolen from the U.S. Office of Personnel Management (OPM) and other agencies.[45]

Cybersecurity challenges also threaten national security. The obvious examples are thefts from government systems containing information vital to national security, such as those committed by Edward Snowden and Chelsea Manning.[46] But cyber attacks on critical infrastructure could be equally devastating to national security. Our defense and security systems depend on roads, utilities, hospitals, and supply chains, all of which depend on secure and reliable ICT. Coordinated cyber attacks on vulnerable critical infrastructure could paralyze commerce, causing catastrophic damage to defense and security.[47]

Finally, global connectivity presents legal challenges for both the public and private sectors. In seeking to bring criminals to justice, individuals and government actors face significant challenges when cybercrime crosses borders.[48] For example, U.S. cyber victims can have difficulty identifying the perpetrators in a foreign country.[49] In addition, they often face difficult questions of jurisdiction and must rely on the host nation's willingness and capability to prosecute the perpetrators.[50]

Innovation. For the U.S. to remain a leader in the industry, ICT firms must continue to outpace global competition in terms of innovation and growth. This, in turn, depends heavily on investment in research and development. There are two principal challenges in this area. One is firms' willingness and ability to invest their own funds; the other is declining federal investment.[51]

Historically, the U.S. government played an important role as a catalyst for innovation in the ICT sector.[52] Research and development resulting in critical technologies such as the Internet and GPS paved the way for much of the innovation that happens in the commercial sector today.[53] The role of the federal government facilitating innovation in the ICT sector has been absolutely critical in supporting a robust ICT research ecosystem, both through direct federal investment in ICT research, and facilitating commercialization and private research investment.[54]

The federal government still has an important role to play. Much of the research and development that happens in the private sector is focused on development.[55] From a microeconomic perspective, this makes sense. Firms are in the business of making money and must develop products and services people are willing to pay for.[56] The pressure to generate short-term returns for investors can act as a disincentive to investing in long-term research activities. Thus, one challenge is the lack of economic incentives at the microeconomic level, creating a "research gap that threatens U.S. leadership in the ICT sector with repercussions for the U.S. economy and national security."[57]

Research is critical to innovation on a macroeconomic level because it stands to benefit the economy, or even society, as a whole. Historically, the federal government, which is not obligated to generate revenues, has invested in or funded research to compensate for the lack of market-based incentives.[58] Changes in policy mean that the U.S. government is not only investing less compared to its own history, but also compared to competitor nations.[59] This means that the U.S. must rely on free market forces to create innovative ICT products and services to support defense and security.[60] Therein lies the second challenge. Because federal business represents a small fraction of total ICT market revenues,[61] market forces alone do not provide enough incentive for firms to engage in a sufficient level of innovation for defense and security applications.

Human Capital. The primary human capital challenge is simply a lack of qualified STEM workers. One reason is that the U.S. has been unable—for a variety of historical, cultural, and policy reasons—to provide enough home-grown STEM workers. In the short term, the obvious answer to alleviate this shortage is to increase the number of qualified foreign workers eligible for H-1B visas in STEM occupations. But the H-1B program, like other immigration policies, is politically controversial: critics allege that the program is a means for industry to hire lower-cost foreign workers to the detriment of American workers.[62]

The facts tell a different story, however. In 2014, when the overall unemployment rate was at 6.2%, the unemployment rate in STEM fields ranged from 2.7 to 3.2%.[63] In the ICT industry, unemployment has hovered at around 4% for the past two years,[64] while the general nationwide employment rates have ranged between 5-6%.[65] These numbers point toward a structural unemployment problem, not a case of cheap foreign labor displacing American workers. Moreover, a shortage of STEM-qualified eligible workers has led to rising wages in the sector.[66] Studies show that H-1B visa holders are earning extremely competitive salaries that are sometimes even higher than those paid to comparable domestic workers.[67]

Why is this happening? Over the past ten years, the U.S. economy added 1.1 million jobs in the IT industry.[68] But in 2013, American universities graduated just over 50,000 students with an undergraduate degree and just over 24,000 with graduate degrees in computer science.[69] Of those graduating with advanced degrees in computer science, about half are non-resident aliens.[70] If job growth continues at the same rate over the next ten years and every single student graduating from a U.S. institution is eligible to work in the U.S., we will still experience a shortage of around 350,000 qualified graduates. If even a fraction of those non-resident alien graduates are ineligible to stay and work, we will experience a brain drain that further exacerbates the shortage of qualified workers.[71]

While the human capital situation is critical for the private sector, it is dire for the public sector. Government employers face fierce competition with private employers for the limited supply of qualified STEM workers, but are limited in the types of financial incentives they can provide. For example, in the ICT industry, the increasing demand for software developers, engineers and other STEM workers has driven wages up beyond a range where the federal government can compete.[72] Even within the government, certain organizations, such as the National Security Agency, have high profile missions that make them more attractive to STEM graduates than other organizations.[73] Moreover, many critical STEM positions in the U.S. are closed to non-U.S. citizens, further reducing the already limited talent pool.[74] The situation will become increasingly difficult as the STEM-qualified government workforce heads into retirement. Federal employers will face a significant knowledge gap if sufficient numbers of younger candidates are not poised to replace aging workers.

Regulatory Policy. One of the major issues affecting the ICT industry today is that U.S. policies and regulatory systems cannot keep up with the pace of technological change. This is a significant challenge because "[r]egulatory design has the potential both to enable and accelerate innovation or to deter it.... In mature industries where core technologies have stabilized, the risk that regulatory design will impede innovation is relatively modest. In other industries that risk is more profound."[75] The challenge lies, therefore, in achieving the right balance between regulation and innovation to produce the desired effects. This challenge is discussed in greater detail in the Selected Essays portion of this report.

Industry Outlook

Short-Term Outlook. Mobile data traffic is expected to grow six fold between 2016 and 2020, growing at an annual compound rate of 42%.[76] Public and private investment in infrastructure will boost ICT industry spending over the near term. Telecommunications operator

investment in mobile and fixed broadband will help boost retail sales of mobile devices and increase demand for broadband enabled content and services. The nationwide broadband initiative, which is discussed in greater detail in the Selected Essays portion of this paper, will also help increase the number of Americans with Internet access and expand the domestic ICT consumer base.

In the near future, the IoT will combine with cloud computing, yielding big data to power decision-making and enabling breakthrough technologies in healthcare, transportation, security and other industries. Accordingly, the ICT subscriber base will expand in the future not just for human users, but also for things; analysts expect a shocking 20 to 50 billion "things" will be connected to the Internet by 2020.[77] Businesses will likely be the biggest users of IoT technology. Analysts estimate up to 40% of all Internet connected devices will support business applications.[78]

Another positive industry signal is found in cloud computing, which is also discussed in the Selected Essays portion of this paper. Cloud computing is one of the industry's fastest-growing segments worldwide.[79] Analysts project strong near term growth with U.S. annualized growth of 4.2%, or $166.2 billion through 2021.[80] Industry growth should also remain strong in the long-term as data storage needs and IT outsourcing drives demand.

A number of social and political challenges portend both exciting opportunities and new threats. The number of simultaneously connected devices will likely result in numerous conveniences such as autonomous vehicles, improved healthcare monitoring, and other smart monitoring devices. Along with convenience, however, these devices will bring new security vulnerabilities. Each new IoT device connected to the network represents another potential point of entry for malicious actors. As discussed in the Challenges section above, risk is already omnipresent for our critical infrastructure, and the recent data breaches at Sony, Target and OPM illustrate these risks to personally identifiable information.[81]

These and other privacy concerns have sent shocks through the industry, especially in Europe. For example, Edward Snowden's revelations about NSA information collection practices are expected to damage U.S. cloud computing providers abroad in the short-term as firms and individuals lose confidence in American firms' data privacy protections.[82] Although this data privacy and security threat looms, the U.S. Federal Trade Commission suggests that IoT legislation today would be premature and is instead encouraging industry to self-regulate.[83] In the short-term we expect to see further public discourse as private and government stakeholders work to address privacy and security issues resulting from the deluge of personal data produced by smart devices and stored in the cloud.

Global Position. The United States is the second largest exporter of ICT goods and, more importantly, is the fourth largest exporter of ICT services.[84] In 2011, U.S. exports of ICT goods and services were higher than those of China—in value added terms—driven partly by the high presence of U.S. ICT services embodied in final products.[85] In the near future, the U.S. ICT industry is well positioned to maintain its competitive advantage because it continues to lead in innovation and new market creation. But security worries and the threat of cyber attacks can cast a dark shadow on the industry. The World Economic Forum warned in January of 2016 that most nations underestimate the damage cyber attacks can wreak on their economies and population.

More unnerving is that "sophisticated government-sponsored espionage exceeds the ability of companies to defend themselves."[86]

Long-Term Outlook. Looking at 2020 and beyond, there are several trends that will factor prominently into the ICT industry's outlook. Opportunities will be found in the world's population growth, the increase in access to banking for those previously unbanked, exponential growth in demand from "things" as well as people, and the massive amount of data the IoT will generate. Specific challenges will be developing policies to deal with sensitive issues like privacy, security, and standardization of technical requirements, among other issues.

In volatile world markets, ICT is among the fastest growing industries. This industry directly creates millions of jobs and is a strong driver of innovation, research, and development around the world. In addition to job creation, some of the largest drivers of GDP growth are increases in broadband penetration and increased mobile data use. The global position of the ICT industry is bright as it continues to drive the delivery of new services and industries, improve service for larger numbers of previously unserved populations and enable business innovation in general.

National Security. National security concerns will remain at the forefront given the connected nature of today's equipment and systems. Once policymakers focus on better understanding the risk to America's critical infrastructure, they will direct their energy toward dealing with a world full of sensors that can collect an incomprehensible amount of data about almost every facet of our world. Unless properly secured, this will generate more data vulnerable to cyber attack. Additionally, despite a number of major attacks, Congress has not passed legislation mandating companies disclose cyber attacks. Disruptive attacks on critical infrastructure or a ransomware attack on a hospital that results in deaths could, however, force the hands of lawmakers and administrators to enact legislation or make policy changes.[87]

Conclusion. The ICT industry is a diverse and dynamic industry characterized by creative destruction and innovation. Growth leaders such as wireless communications, cloud computing, Internet search, and online advertising are supplanting former industry leaders such as wireline communications as increasing numbers of people connect in various ways. The ICT industry is positioned to maintain dominance in the near and long term due to a supportive economic environment and relatively stable and robust macroeconomic fundamentals. The near future of the ICT industry will be driven by two main forces, the IoT and an expanding subscriber base for wireless data services. Long term, 2020 and beyond, the industry will be driven by data demands of a growing world population, use of big data that people and things generate, and the increased policy complexities that come along with such expansion.

Government Goals and Role

Innovation. While good public policy initiatives can encourage private research and development, there will always be a role for the federal government in the ICT industry. However, the landscape has changed dramatically since the DoD birthed ARPANET and GPS. According to a 2014 National Science Foundation (NSF) report, the federal public sector's leading role in research and development investment was supplanted by the private sector in 1980, and the gap

between the two has widened and stabilized over time. The most recent data (2013) shows that the federal government made up 27% of American research and development investment compared to 65% from the private sector.[88] To many in the defense community, this is a troubling trend that demands action.

To that end, the President's 2017 budget request contains a 4% research and development increase over 2016 levels.[89] But even with increased federal investment, the public-private investment gap is unlikely to close. In a free market economy, this trend is logical and should be embraced. Private research and development investment can be complementary to DoD investment. Further, private investment catered to meeting consumer needs boosts living standards and American prosperity. That prosperity enables funding (*i.e.* tax revenue) for enhanced national security.

The federal government's role in innovation should take a more nuanced, hybrid approach. One example of this type of approach is the Defense Innovation Unit Experimental (DIUx). As part of the "third offset strategy" centered on technology improvements, Secretary of Defense Carter unveiled DIUx in April 2015, aiming to "build bridges and rebuild bridges and renew trust . . . to learn how, in the years to come, a new level of partnership can lead to great things."[90] DIUx opened its doors in Silicon Valley four months later with the stated purpose to "strengthen existing relationships and build new ones; help scout for new technologies; and help function as a local interface for the department."[91] DIUx offers real promise in several areas to include harvesting best practices in innovation and technology development, and raising DoD understanding of the ICT industry (and vice versa).

Human Capital. While immigration reform remains politically controversial, we recommend policy changes to alleviate the immediate shortage of STEM qualified workers.[92] Congress should immediately pass legislation relaxing H-1B visa quotas for graduate students in STEM fields. This would have two benefits. First, since there is no limit on the number of foreign students in our universities, we will see an increase in enrollment if we hold out the promise of greater chances for employment after graduation.[93] Second, we can retain the most qualified foreign students and avoid the brain drain discussed in the Challenges section, above. In short, immigration reform is the most cost efficient way to alleviate the shortage of STEM experts in the short term.

Cybersecurity. The U.S. government's closest ally within the cyber domain should be the ICT industry. Just as we work closely with our NATO and other treaty allies to defend the four domains—land, air, sea, and space—we need the ICT industry to participate in the defense of the fifth domain, cyberspace.[94] To achieve a national cyber defense model with depth, we need government and industry to share more effectively what Allison Bender of the International Association of Privacy Professionals (IAPP) calls "cyber-threat intelligence."[95] Both government and industry have a vested interest in securing our nation and reducing cyber related risks. Only together are we optimized to close the seams in our information and communications infrastructure.

Acquisition Reform. While many aspects of the federal acquisition process could benefit from reform, there are three that have a particularly disproportionate impact on government ICT

needs. The first is the acquisition system's complexity and lack of agility, the second involves inappropriate contracting strategies, the third is poor requirements definition and management. All three make it difficult for the federal government to acquire and integrate new technology.

ICT firms are not shy about their frustration with the federal acquisition system.[96] A recent Brookings Institute research paper found that Silicon Valley executives saw significant barriers to entry in defense business because of an acquisition system that "neither works in their favor nor is remotely consistent with the speed and agility these companies need to simultaneously compete in broader and in many cases more liquid global technology markets."[97] The process creates a disincentive for firms to compete for federal business, leaving potentially game changing technologies out of reach.[98] Worse, the federal government can be its own worst enemy. Tight budgets and a reluctance to embrace new approaches create a disincentive for federal workers to sign off on up-front capital outlays, even where doing so would result in dramatic sustainment cost savings.[99] Support for legacy systems not only costs more than upgrading to new systems, but it also exposes the government to increased cybersecurity risk.[100]

Government and industry leaders echo the position taken by the National Defense Industry Association (NDIA) that the government's preference for Lowest Price Technically Acceptable (LPTA) contracting is often misapplied and harmful.[101] Whereas fuel and traditional office supplies (*e.g.*, paper) are true commodities appropriately aligned for LPTA contracting,[102] many ICT solutions are aligned with best value (tradeoff) contract strategies. Along these lines, the Government Accountability Office (GAO) found that the "DoD's ability to clearly define requirements and its knowledge of potential vendors were key factors that underpinned decisions about whether to use tradeoff or LPTA" and such factors were generally consistent with federal acquisition guidelines.[103] In other words, if we know (and can articulate) exactly what we need and quality and offerings are standardized across vendors, LPTA is appropriate. That is rarely the case in the ICT arena. Indeed, the first key factor identified by GAO—requirements clarity and definition—is very challenging with ICT.

Regarding requirements management, in order to take advantage of emerging technologies or methods of delivering technology-based solutions, the government must shift away from a focus on buying physical things, such as servers, routers, and licenses, and instead embrace a consumption-based pricing model aligned with the ICT market's direction.[104] With advances such as cloud-computing and subscription-based software licensing, the ICT industry is moving toward a more dynamic purchasing model that allows for adjustable scalability, predictable pricing, and easy modernization, while at the same time protecting security.[105] Although federal policymakers have encouraged agencies to capitalize on the advantages these new models offer, agencies have been slow to embrace them, while pouring significant funds into maintaining legacy systems.[106]

Regulatory policy. Much of the regulatory framework governing the ICT industry is outdated and simply does not fit the digital world; it is no longer appropriate to try to apply the analog principles to a digital world. Bold changes are required to prevent our regulatory system from hindering growth and innovation in the ICT industry. The goals and role of government in the context of specific regulatory issues are discussed in the Selected Essays portion of this report.

SELECTED ESSAYS ON MAJOR ISSUES

Privacy, Encryption, and the Risks of the FBI-Apple Dispute for the ICT industry
by Brian Greaney

We are not "going dark." Despite the growth in the use of privacy and encryption technologies since the late 1990s, governments around the world have experienced what some describe as a "golden age of surveillance" driven by new device-driven streams of unencrypted data.[107] In the United States, partnerships between the private sector and the government have traditionally been crucial for surveillance, especially when the post 9-11 political climate allowed for more intrusive eavesdropping measures.[108] However, elements of this partnership are now in crisis. This is exemplified by the FBI-Apple dispute,[109] bringing to fruition a debate on privacy and encryption that has raged for decades.

Over the years, governments have seldom had a consistent policy direction on encryption and privacy. During the evolutionary period of encryption-related policymaking, some elements of the U.S. Government took a pro-encryption stance—developing, applying, and reaping the rewards of technologies such as The Onion Router (TOR)[110] (a communications anonymizer), that kept individuals' information and identities safe from prying eyes.[111] On the other end of the spectrum, the Clinton Administration very publicly failed in its efforts to mandate "Clipper Chips,"[112] which would have provided the government access to encrypted data in mobile technologies.[113]

No single incident influenced the debate over privacy and encryption more than the Snowden leaks. Governmental entities, the so-called "good guys," who had wanted individuals and companies to trust them, became the object of much more widespread private-sector suspicion.[114] It is likely true that "Apple's design of an operating system impervious even to its own efforts to crack it was a response to a global loss of trust in the institutions of surveillance oversight."[115] By deploying an encryption system that the provider itself could not hack, Apple sent an implicit message to all users (and potential users) worldwide: "You don't have to trust us; you don't have to trust the democratic oversight processes of our government. You simply have to have confidence in our math."[116]

We risk driving firms towards solutions like the one adopted by Apple, and users towards foreign software.[117] ICT firms who can hack their own encryption systems now operate at their peril. In 2013, faced with a court order and an FBI instruction to "defeat his own system," the Lavabit encrypted email system's founder refused and closed his company. He then warned that he "would strongly recommend against anyone trusting their private data to a company with physical ties to the United States."[118] Moreover, firms are increasingly incorporating end-to-end encryption. When, in April 2016, the WhatsApp messaging platform moved to end-to-end encryption, the content of one billion users' messages went beyond the potential reach of court orders.[119] They also became much harder for authorities to hack.

During this debate, experts have been near unanimous in their explanation that it is not possible to have both secure encryption and a backdoor available to authorities. [120] Past examples of poor security raise legitimate concerns that backdoors could not be effectively locked and the

keys successfully hidden. In 2004-2005, the Greek government was hacked through a cellphone vulnerability that it had insisted Vodafone install.[121] In 2009, Chinese hackers stole a Google database of users subject to Foreign Intelligence Surveillance Act (FISA) orders (legal rulings which were themselves classified), providing China with information on U.S. targets such as spies, diplomats, suspected terrorists and agents of other governments.[122]

The most fundamental flaw in the FBI's argument with Apple is that it lacks strategic perspective. Despite the best efforts of proponents of the FBI's view, a simple weakness remains: "Encryption is math. Foreigners can do math."[123] While the FBI is in a position to encourage American firms to weaken encryption, it has no power to ban foreigners from filling the resulting gap, or to ban users from migrating to those systems.

A house divided against itself cannot stand. The jury is out on whether or not government and industry will work with or against each other on this issue in the future.[124] Government can move to repair the damage by 1) minimizing national cybersecurity vulnerabilities through the rejection of requirements for backdoors to encryption, 2) accepting the reality that malfeasors will find access to strong encryption regardless of U.S. government policy, and 3) collaborating to rebuild trust with U.S. firms. This approach would bolster confidence in our future level of national resilience in cyberspace, and also in the future economic strength and technological innovation of the U.S. ICT industry as a whole. In a more trusting environment we might also be able to restore the regulatory predictability essential for ICT firms to confidently take business decisions that strengthen the industry, and lessen the risk of quick legislative action based on emotional and politically seductive arguments about terrorism.

Cloud Computing by Lamont Atkins

Cloud computing has emerged as a game changer for businesses and consumers as it addresses major challenges facing the ICT industry. Cloud computing provides scalable, adaptable, and cost effective capabilities as services using proven Internet technologies. It affords business consumers the opportunity to accelerate innovation, increase competitiveness, and drive overall IT costs down. As cloud computing has rapidly matured over the years, the traditional concerns of security, trust, data management, and control have been significantly reduced and the technology is poised to be an expansive growth segment of the ICT industry.

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[125] NIST also identified three models for cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).[126] Each mode provides a different level of capability to an organization. In an IaaS environment, an organization leases space on the provider's computing equipment including storage space, servers, and network components to support its operations.[127] In addition to leasing infrastructure, PaaS provides an operating system and application hosting as a streamlined service.[128] SaaS is a software distribution model allowing companies to access programs or applications from the provider via

the Internet.[129] Each service model is scalable and allows a company the opportunity to enter the market at their pace and expand on a timeline aligned with their IT strategy.[130]

As a subsector of the ICT industry, cloud computing services have entered a hyper growth stage due to wider adoption. Allied Market Research estimates that investment in cloud services will grow from $209.9 billion in 2014 to $555 billion by 2020, representing a compound annual growth rate of 17.6 percent through the end of the decade.[131] Microsoft, Oracle, and Amazon are leading the surge by shifting more of their focus and resources to cloud services. Oracle paid its sales force a 7x multiplier on cloud deals in the first quarter of 2015, an indicator of its drive to achieve early success in a lucrative market where scale will be a key factor for the winners.[132] Microsoft CEO, Satya Nadella, vowed that Microsoft would have $20 billion in annual cloud revenue by the middle of 2018.[133] Amazon has made cloud ubiquitous, and achieved $4.6 billion in revenue in 2014, and reached $6.2 billion in 2015, with a growth rate of 49 percent.[134]

Cloud computing adoption is growing in the federal sector as well. According to an International Data Corporation report, "federal government spending on cloud will increase from $6.66 billion in fiscal year 2015 to $11.46 billion in fiscal year 2019.[135] Currently, there are 32 authorized commercial cloud service offerings in a variety of configurations with varying levels of security that are FedRAMP compliant and available for federal agency deployment.[136] FedRAMP deploys a 'do once, use many times' framework for conducting security assessments of potential cloud service providers.[137] This standardized, government-wide process improved the trustworthiness, reliability, consistency, and quality of the cloud provider authorization process and has ignited the use of cloud solutions across the federal government.[138]

The Department of Defense accounts for 37% of the federal agency spending on cloud services for Fiscal Year 2016.[139] The DoD's move to cloud computing can be characterized as a fast follower rather than early adopter. Fast followers are generally not as quick to adopt unproven technologies to avoid much of the risk associated with the new technology. The fast follower approach is appropriate given the DoD's higher risk profile due to national security and the dependency of trusted data. The loss of the confidentiality, availability, or integrity of a DoD system could cost lives. However, as cloud services have expanded over time and become more trusted and cost-effective, organizations within the DoD have relied more on the cloud, permitting them to focus resources on their primary mission instead of deploying and maintaining information technology.[140] There are currently several deployments of commercial cloud implementations within the DoD and that number is growing monthly.[141]

Wireless Spectrum Management by Fernando Guadalupe

On January 29, 2015, the Federal Communications Commission (FCC) completed an auction of Advanced Wireless Service (AWS) licenses in the AWS-3 bands. This auction raised over $44 billion in bids, with 31 bidders winning over 1,600 licenses to expand and enhance the delivery of wireless services.[142] This auction attests to the growth in commercial wireless broadband services, including smart phones and tablet computers, as well as increases in government missions using radio frequency spectrum. It also serves as a reminder of how crucial spectrum use is to the economic and security fitness of the United States. Therefore, it is important

that the United States establishes an agile 21st century policy for spectrum management to drive economic growth and further enhance America's national security posture.

The electromagnetic spectrum is a natural resource that demonstrates some of the properties of what economists call a common good.[143] That is, while its use is free, each user has little to no incentive to use the spectrum efficiently. Unlike other natural resources that are consumed by use, spectrum is not. It becomes readily available for reuse once its previous user stops using it. However, spectrum is scarce, as only a portion of it is usable at any given time. It is in this scarcity that the value of spectrum is realized. The U.S. government and the ICT industry together spend more than $300 billion a year on capital projects that expand wireless communications coverage, enhance services, and create jobs.[144] This investment is most valuable to the national economy when spectrum is available, efficiently used, and well-managed.

The Communications Act of 1934[145] and the Commercial Spectrum Enhancement Act of 2004[146] (CSEA) provide the regulatory framework. The National Telecommunications and Information Administration (NTIA) manages the federal government's use of the spectrum while the FCC manages all other uses.[147] Although spectrum management has been practiced in the United States for over 100 years,[148] it is still very much a work in progress because of changing technology and growing demand for the spectrum. As a result, a modern approach is necessary to create an active and relevant 21st century spectrum use policy. This modern approach to spectrum policy needs to shift away from a command and control driven regulatory process to a market driven one distinguished by a framework that allows the free trade of spectrum, incentive-driven auctions to repurpose spectrum, and transitions from static to dynamic spectrum sharing.

A market driven process allows for spectrum rights that can be freely traded largely independent of any FCC administrative control unleashing market forces to keep up with technological advancements at a more rapid pace.[149] Along with this, auctions should continue, but they need to mature into incentive-driven auctions where increased re-allocation from incumbent frequency holders meets market-driven needs. The incentive auction also greatly benefits consumers by easing congestion on wireless networks, laying the groundwork for "fifth generation" (5G) wireless services and applications, and spurring job creation and economic growth.[150] Regarding spectrum sharing, moving licensed users from one portion of the spectrum to another will soon become impossible with the advent of the Internet of Things where billions of additional devices will overwhelm portions of the spectrum.[151] As a result, there is an obvious desire for underutilized spectrum. A solution may lie in dynamic sharing where coordination systems allow an enabled device to query a frequency database to automatically select an available frequency to use.[152]

The United States needs to make spectrum use policy a priority right now. A policy that applies a modern approach to spectrum management will serve as an economic driver for very much needed growth. Thus, the U.S. economy can capitalize on the efficient use of the spectrum and enlarge the resource base necessary for a robust and effective national security posture.

Capacity Building for Telecommunication Operators by Adamu Abubakar

Human resources are the most valuable factor in production and the most vital asset for any organization, particularly when it comes to technical manpower. The vital role the telecommunications industry plays today in providing services in sectors like finance, energy, health, education, and commerce require constant awareness by all actors in the industry. The critical infrastructure for the telecommunications industry is multifaceted and needs a multi-pronged approach to address the security challenges facing the industry in human resource development. The telecommunications industry is highly technical in nature and requires operators with high technical skills as well as knowledge to address the current and future security challenges. Key sectors of the U.S. economy rely heavily on the telecommunications infrastructure for their day-to-day operations; the role of human resource development is vital in the industry.

The multi-billion-dollar telecommunications industry in the United States is having challenges fielding a qualified workforce. Many companies rely on H-1B visas to recruit technical staff.[153] This means that the U.S. education system needs to spend more funds on technical education and also encourage students to study the sciences by giving them scholarships. In today's world of telecommunications technology, the importance of human development in organizations and society will strengthen the human and institutional capacity to resolve threats and prevent attacks on telecommunications infrastructure.

Telecommunications companies could spend more money on new work skills, rebuild the old skills and create a link between organizations to source for specific skills when the need arises. In addition, more funds could be provided to institutions of higher learning and innovation centers, so that talents can be discovered early and be trained to meet the industry challenges. The industry could also organize training interventions to build capacity and tackle emerging challenges.

In view of the new trends in the industry and fast changing nature of the mobile networks, more funds could be allocated to research, and knowledge sharing, as well as providing training services to clients. Support centers could also be established to enhance capacity on how to handle emergencies. The objective is to improve human capacity building within the work force, including senior managers, regulators, operators, service providers, and government agencies. This will promote a sustainable and proactive culture of telecommunications security.

Implementation of the National Broadband Plan by Edward Paglee

In 2009, recognizing the vital importance of broadband availability across the nation, Congress directed the FCC to develop a National Broadband Plan to ensure every American has "access to broadband capability." Released on March 17, 2010, the plan set out a roadmap for initiatives to stimulate economic growth, spur job creation, and boost America's capabilities in education, health care, homeland security and more.[154] However, six years later, the U.S. ranks only 41st in the world in Internet bandwidth per user.[155] World rankings for both fixed-broadband and mobile-broadband subscriptions per population were 20th and 17th, respectively.[156] The FCC's 2016 Broadband Progress Report found that ten percent of all Americans (34 million people) lack access to high-speed broadband, and this percentage increases to 39 percent for rural Americans.[157] Therefore, recognizing how important broadband access is to users, the ICT

industry, and all other industries that leverage the Internet for productivity gains, it is worth examining whether or not the National Broadband Plan is structured to achieve its goals and simultaneously incentivize efficient investment by U.S. companies.

Three of the six goals of the plan focus on broadband deployment. First, the plan encourages private investment to provide at least 100 million homes affordable access to download speeds of at least 100 megabits per second (Mbps) and upload speeds of at least 50 Mbps by 2020.[158] With incumbent communications companies all offering full or hybrid fiber broadband in much of the United States, meeting the goal appears to be a forgone conclusion.[159] Even absent fiber-to-the-home connections, upgrades to advanced cable communications protocols known as Data over Cable System Interface Specification version 3.1 (DOCSIS 3.1) will likely deliver speeds well over 100 Mbps using much of the existing cable infrastructure.[160]

Until now, fiber-to-the-home has been the preferred technology for delivering this capability, but has not proven to be an investment that all U.S. communications companies find profitable. For example, the expense of replacing old copper lines with fiber led Verizon to stop building its fiber-to-the-home network in new regions in 2010.[161] But fiber-optic cable is still vital, as it comprises the majority of the Internet backbone.[162] The plan's other goal of providing affordable access to at least one gigabit per second service to every community in order to anchor institutions such as schools and government buildings is also more likely to be dependent on a fiber connection. Several communities now have gigabit broadband through combinations of fiber, cable and traditional wired networks, and companies including AT&T, Google and CenturyLink are taking the lead to continue fiber deployment.[163]

The stated mobile broadband goal of the National Broadband Plan is that the U.S. should "lead the world in mobile innovation, with the fastest and most extensive wireless networks of any nation."[164] With both AT&T and Verizon networks covering over 94% of the U.S. geography,[165] access is not an issue: The World Economic Forum ranks the United States 17th for mobile-broadband subscriptions per population.[166] In fact, according to OpenSignal's *State of Mobile Networks* report, fourth generation (4G) coverage in the United States is among the world's best with 4G subscribers able to see an LTE signal 81 percent of the time—only seven other countries are comparable.[167] However, although LTE-advanced networks have pushed the upper boundaries of download speed beyond 30 Mbps, the U.S. is not leading the way as evidenced by the 4G average of only 9.9 Mbps, well short of the global download average of 13.5 Mbps.[168]

Particularly in the arena of fixed broadband, it is clear that for companies to continue to make the significant capital investment required to expand fiber rollout, there must be enough profit motive to sustain this momentum. The "light touch" policy that was embraced in the early years of the Internet[169] is in danger of suffering under the weight of new restrictive regulations. The 2015 FCC rules governing Open Internet and Net Neutrality[170] require a second look. The intent of the rules is to ensure that consumers and businesses have access to a fast, fair, and open Internet. But if the burden of these regulations remains overly costly to the industry, then instead, Net Neutrality will induce less incentive for the industry to continue expanding their networks. Rather than further governance through restrictive regulatory process, success of broadband innovation and continued expansion across America may better be left to the multi-stakeholder innovation-driven process that created the technology in the first place.

Six years after the release of the National Broadband Plan, it appears time for a thorough update. The plan is correct in that broadband is the foundation for economic growth, job creation, global competitiveness and a better way of life. But the goals that might have seemed audacious in 2010, have largely been eclipsed by the continued advancement of technology. As the FCC continues to focus on the rural broadband gap in its annual broadband progress reports, it appears clear that this gap continues to close. Disruptive technologies such as gigabit wireless and 5G mobile networks seem poised to eliminate all access issues in the very near future. But the plan needs to shape a policy that fosters continued investment in both research and development, as well as further network deployment. This requires realignment of incentives and removal of counter-productive regulation to spur additional risk taking. While the authors of the original plan may look to the current state of broadband in the nation and declare success, it is instead more probable that success was realized despite the plan, as a byproduct of simple entrepreneurship and innovation.

Net Neutrality and Federal Communications Policy by Genevieve Sapir

Going back centuries, western civilization has embraced the principle that members of the public should have legally-mandated, non-discriminatory access to those goods and services society deems essential to communications and commerce. This principle holds true even in the digital age. The future of American communications regulatory policy should be firmly grounded in the principle of non-discriminatory access to broadband Internet services, which are the essential instruments of commerce that drive opportunity, growth, and participation in democracy. But there should be a regulatory *quid pro quo*: as we bring broadband Internet service under federal regulatory authority, we should release all other communications services from regulation. Competition for voice and video is thriving and no longer needs the legacy of regulation that it once did. Accordingly, federal communications policy should be focused on the only remaining actors with the power and incentive to foil competition: the broadband network owners.

Although proponents of capitalism eschew regulation as anathema to free market principles, access to transportation and communication networks is the bedrock of our economic system. Discussing the importance of common carrier regulation to the rise of capitalism, researcher Mark Cooper observed that "the principle of nondiscriminatory access to the means of communications and commerce has been part of the DNA of capitalism since its birth…the movement of goods and ideas is essential to the success of the capitalist economy and the democratic polity."[171] He further observed that "[p]roviding for open and adequate highways of commerce and means of communications were critical to allow commerce to flow, to support a more complex division of labor, and to weave small, distant places into a national and later global economy."[172]

The major impediment to open Internet access is that a small number of large, diversified companies control the networks that provide broadband services. In major markets, consumers may have a choice, but they are usually limited.[173] Consumers in smaller markets and rural areas have even fewer choices. These market conditions are unlikely to change. Due to high barriers to entry and economies of scale, the market will only ever be able to support a small number of communications networks. [174] If nothing else, the telecommunications boom, bust, and then consolidation of the late 1990s and early 2000s, illustrated this point.[175]

But lack of competition in network access is only part of the problem. Broadband service providers are not just providers of network access, they also compete with third-party providers selling services on the network. Increasingly complex vertical and complementary relationships create incentives to exclude or hinder non-affiliated entities from offering competing services.[176] For example, major market broadband providers like Comcast and Verizon provide both telephone and video services. Many offer packages with significant discounts if the consumer purchases a bundle of services. This is not necessarily bad; consumers can benefit by receiving lower prices for goods and services. But if network providers misuse their control over the network to edge out competition, the result is bad for consumers. Over time, in the absence of meaningful competition, consumers will see fewer choices and rising prices.

But above all, non-discriminatory access to broadband networks is necessary because it promotes the virtuous cycles of investment and innovation that are the building blocks of economic growth. To some, this position is counter-intuitive. Opponents of regulating broadband Internet service argue that regulation stifles innovation and that classifying broadband service providers as common carriers will reduce their investment in the networks.[177] Opponents are justifiably concerned about the chilling effect of regulation; however, they fail to distinguish between the effect of regulation on those who innovate and invest in the physical network vice those who innovate and invest in services provided over the network. Net neutrality is designed to protect and promote the "virtuous cycle" that drives innovation and investment.[178] A great deal of that innovation and investment is generated by third-party providers who depend on broadband Internet access to sell, develop, or deliver their services. Rather than stifle investment and innovation as some argue, non-discriminatory access actually has the opposite effect: it allows third-parties to compete where they might otherwise have been forced out. In other words, non-discriminatory access creates the necessary conditions for innovation to happen at the edge.

Whereas the FCC was right to mandate open access to the Internet, it took a wrong turn, when it determined broadband Internet services to be telecommunications services. Dating back decades, the FCC has based its regulatory scheme on the distinction between "pure communications" and "pure data processing" services.[179] Over time, and in response to statutory amendments, the FCC made important distinctions between telecommunications subject to common carrier regulation (telephone) and "information" services (Internet) exempt from regulation. This made sense when telecommunications services were the core services provided over the networks and all other services were secondary. But that distinction no longer makes sense. Today, information services, not telecommunications services, are the core services carried over the networks. This is largely because the different types of communications services–voice, video, and data–no longer depend on separate networks for transmission. The ability to use or provide any of these services depends only on the ability to send data packets across broadband networks. Accordingly, now that voice communications are no longer the mainstay of our communications network, it no longer makes sense to base our model of regulation on access to those services.

Moreover, the fundamental justification for regulating voice and video services–lack of competition–no longer exists. Before consumers could easily access voice and video services through broadband Internet connections, they were dependent on telephone and cable television providers building infrastructure to reach their homes. They relied on federal regulators to ensure

that these service providers, which had little to no competition, provided quality service at just and reasonable rates. But the availability of voice and video services through the Internet has changed all of that.

Rather than trying to jam modern Internet protocol-based services into the legacy telecommunications regulatory model, the right approach is to create a new Digital Communications Act tailored to the specific needs of the Internet Age. The proliferation of broadband Internet service eliminated the network effect that inhibited competition in voice and video. This warrants an entirely new regulatory paradigm under which we regulate broadband Internet service providers as common carriers, but completely deregulate voice and video services. In essence, federal policy should set the bounds for fair and open broadband access, but within those bounds, innovative service providers would have a very large sandbox in which to innovate, invest, and compete for customers.

Conclusion

Today, the ICT industry is everywhere and touches almost every aspect of our lives. With the promise of the Internet of Things, its footprint is projected to grow even larger. This is good news for the American economy and national security. We can grow our standard of living, improve quality of life, and provide national security in ways we never dreamed possible. But there is a trade-off. We risk a loss of privacy and will have to work increasingly hard to secure sensitive data.

We, the Eisenhower School's ICT seminar, conclude that effective collaboration between the ICT industry and the U.S. government can promote both economic growth and national security. For its part, the federal government should embrace policies that include, at a minimum, immigration and education reform to address our shortage of science, technology, engineering, and mathematics (STEM) workers, as well as a renewed commitment to research and development funding and federal acquisition reform. We must also take a hard look at regulatory policies to make sure they not just allow, but encourage, the industry to innovate and grow further. And as cyber security emerges as a dominant threat to both national security and individual privacy, we must be forward-thinking in crafting new solutions as partners with industry.

This is no small task: the ICT industry will always be moving faster than the pace of government. Accordingly, more than ever before, we must embrace policies that are flexible, dynamic, and do not stand in the way of innovation.

APPENDIX

NAICS	ICT Markets
Hardware	
33411	Computer and Peripheral Equipment Manufacturing
33421	Telecommunications Networking Equipment Manufacturing
33422	Communications Equipment Manufacturing
42343	Computer Equipment and Software Wholesaling
Software	
51114	Database and Directory Publishing
51121	Software Publishing
51913	Internet Publishing and Broadcasting and Web Search Portals
Communications	
51711	Wired Telecommunications Carriers
51721	Wireless Telecommunications Carriers
51741	Satellite Telecommunications
51791	Other Telecommunications
Services	
51821	Data Processing, Hosting, and Related Services
54151	Computer Systems Design and Related Services
81121	Electronic and Precision Equipment Repair Services

ENDNOTES

[1] Management consultant Peter Drucker famously described automobile manufacturing as the 'industry of industries' in 1946 due to its scale and impact on the overall economy. The automobile industry also led thinking in management science and industrial engineering. The modern ICT industry is similarly large in scale, has enormous impact on the economy, and leads thinking in innovation. Peter F. Drucker, *The Concept of the Corporation* (New York, NY: John Day Company, 1946): 149.

[2] The North American Industry Classification System (NAICS) is used by Federal statistical agencies to classify establishments related to the U.S. business economy. IBISWorld market research subdivides several ICT-related NAICS codes into specific markets with a letter designator. From United States Census Bureau, "North American Industry Classification System," accessed 31 January 2016, www.census.gov/eos/www/naics. Also from IBISWorld, "Search Results: Industry Market Research," accessed 31 January 2016, www.ibisworld.com/search.

[3] "Computer Manufacturing in the US," IBISWorld Industry Report 33411a, April 2016, accessed May 16, 2016, www.ibisworld.com; "Computer Peripheral Manufacturing," IBISWorld Industry Report 33411b, October 2015, accessed May 16, 2016, www.ibisworld.com; "Telecommunications Networking Equipment Manufacturing," IBISWorld Industry Report 33421, April 2016, accessed May 16, 2016, www.ibisworld.com; "Communications Equipment Manufacturing," IBISWorld Industry Report 33422, March 2016, accessed May 16, 2016, www.ibisworld.com; "Recordable Media Manufacturing," IBISWorld Industry Report 33461, December 2015, accessed May 16, 2016, www.ibisworld.com.

[4] "Computer Manufacturing in the US," IBISWorld Industry Report 33411a.

[5] Ibid.

[6] Samantha Nelson, "Apple's Premium Pricing Strategy and Product Differentiation," Market Realist, February 6, 2014, accessed May 13, 2016, http://marketrealist.com/2014/02/apples-premium-pricing-strategy-product-differentiation/.

[7] See note 3, supra.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] "Software Publishing in the US," IBISWorld Industry Report 51121, December 2015, accessed May 16, 2016, www.ibisworld.com; "Search Engines in the US," IBISWorld Industry Report 51913a, November 2015, accessed May 16, 2016, www.ibisworld.com; "Internet Publishing and Broadcasting in the US," IBISWorld Industry Report 51913b, September 2015, accessed May 16, 2016, www.ibisworld.com.

[12] "Software Publishing in the US," IBISWorld Industry Report 51121.

[13] Ibid.

[14] "Search Engines in the US," IBISWorld Industry Report 51913a; "Internet Publishing and Broadcasting in the US," IBISWorld Industry Report 51913b.

[15] "Software Publishing in the US," IBISWorld Industry Report 51121.

[16] See note 11, supra.

[17] Ibid.

[18] "Wireless Telecommunications Carriers in the US," IBISWorld Industry Report 51721, August 2015, accessed May 16, 2016, www.ibisworld.com.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] *See* Benjamin Snyder, "Google Has a Plan to Revolutionize Your Cell Phone Service," *Fortune*, March 2, 2015.

[24] "Wired Telecommunications Carriers in the US," IBISWorld Industry Report 51711c, September 2015, accessed May 16, 2016, www.ibisworld.com.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] "Satellite Telecommunications Providers in the US," IBISWorld Industry Report 51741, September 2015, accessed May 16, 2016, www.ibisworld.com.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] "IT Consulting in the US," IBIS World Industry Report 54151, October 2015, accessed May 16, 2016, www.ibisworld.com.

[39] Ibid.

[40] Ibid.

[41] "Data Processing and Hosting Services in the US," IBISWorld Industry Report 51821, March 2016, accessed May 16, 2016, www.ibisworld.com.

[42] "The Gig Economy, Smooth Operators," *The Economist* 418, no. 8977, February 20, 2016, 63-64.

[43] Virginia Harrison and Jose Pagliery, "Nearly 1 Million New Malware Threats Released Every Day," CNN Money, April 14, 2015, accessed May 16, 2015, http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/.

[44] Steve Morgan, "The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics," Forbes, October 16, 2015, accessed, May 16, 2016, www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#5e14940810b2.

[45] Patricia Zengerle, "Millions More Americans Hit by Government Personnel Data Hack," Reuters, July 9, 2015, accessed May 16, 2016, www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709#D8iMKoaUjKxmMVkr.97.

[46] Ian Simpson and Medina Roshan, "U.S. Soldier Manning Gets 35 Years for Passing Documents to WikiLeaks," Reuters, August 21, 2013, accessed May 14, 2016, www.reuters.com/article/us-usa-wikileaks-manning-idUSBRE97J0JI20130821; Barton Gellman, Aaron Blake, and Greg Miller, "Edward Snowden Comes Forward As Source of NSA Leaks," *Washington Post*, June 9, 2013, accessed May 14, 2016, www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

[47] The challenge of securing America's critical infrastructure from cyber attack is overwhelming. According to the Department of Homeland Security's Critical Infrastructure web page there are more than 100,000 Defense Industrial Base companies and subcontractors; 6,413 power plants (62 nuclear); 160,000 public drinking water systems; 16,000 publicly owned wastewater treatment systems; 87,000 dams; 400,000 registered food manufacturing, processing and storage facilities, 450 commercial airports, 19,000 additional airports, 361 ports, and millions of miles of rails, roadways, bridges, tunnels, and fiber cables in the United States. "Critical Infrastructure Sectors," Department of Homeland Security, May 16, 2016, www.dhs.gov/critical-infrastructure-sectors. Exacerbating the challenge is that more than 80 percent of all critical infrastructure is privately owned. No one-size-fits-all solution exists for protecting this infrastructure. Mary Catherine Ott, "New Legislation in Senate to Create 'Cyber Guards,'" The National Guard Association of the United States blog, March 22, 2013, accessed May 16, 2016 http://ngaus.org/blog/13/04/new-legislation-senate-create-cyber-guards#sthash.6bB9tQvl.dpuf.

[48] *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, (CRS Report No. R41927) (Washington, DC: Congressional Research Service, January 17, 2013), 1.

[49] Ibid., 14.

[50] Ibid., 10-11.

[51] John C. Anderson and Danielle Coffey. "U.S. ICT R&D Policy Report: The United States: ICT Leader or Laggard?" Telecommunications Industry Association, September 15, 2011, accessed May 13, 2016, www.tiaonline.org/sites/default/files/pages/TIA%20U%20S%20%20ICT%20RD%20Policy%20Report.pdf.

[52] "Research Ecosystem," Telecommunications Industry Association, accessed May 13, 2016, www.tiaonline.org/policy/research-ecosystem.

[53] Thomas Farnan, "How Dwight D. Eisenhower Invented the Internet—and the Desktop Computer," Forbes, September 2, 2014, accessed April 10, 2016, www.forbes.com/sites/realspin/2014/09/02/how-dwight-d-eisenhower-invented-the-internet-and-the-desktop-computer/2/#71fe3cc23020.

[54] Anderson and Coffey.

[55] "Research Ecosystem," Telecommunications Industry Association.

[56] Ibid.

[57] Ibid.

[58] Farnan.

[59] Stephen Ezell, "University Startups Conference Showcases Latest ITIF Tech Transfer and Commercialization Policy Proposals," The Innovation Files, April 07, 2016, accessed April 10, 2016, www.innovationfiles.org/university-startups-conference-showcases-latest-itif-tech-transfer-and-commercialization-policy-proposals/.

[60] Sandra I. Irwin, "Defense Technology at a Crossroads: Can the Pentagon Regain Its Innovation Mojo?" NDIA Business and Technology Magazine, April 2015, accessed May 13, 2016, www.nationaldefensemagazine.org/archive/2015/April/pages/DefenseTechnologyAtaCrossroadsCanthePentagonRegainItsInnovationMojo.aspx.

[61] Ginger Pinholster, "White House: Modest 2015 R&D Budget Proposal, but with a Twist," American Association for the Advancement of Science, March 03, 2014, accessed April 10, 2016, www.aaas.org/news/white-house-modest-2015-rd-budget-proposal-twist.

[62] Michael Hiltzik, "A Phony STEM Shortage and the Scandal of Engineering Visas—how American Jobs Get Outsourced," *Los Angeles Times*, February 26, 2016, accessed April 17, 2016, www.latimes.com/business/hiltzik/la-fi-mh-the-scandal-of-engineering-visas-20160226-column.html.

[63] Nager and Atkinston, citing, "Household Data Annual Averages (Unemployed Persons by Occupation and Sex, 2014)," Bureau of Labor Statistics, accessed April 3, 2015, www.bls.gov/cps/cpsaat25.pdf.

[64] Bureau of Labor Statistics information for the "Information Industry" was used to calculate this unemployment rate. "Table A-14. Unemployed Persons by Industry and Class of Worker, Not Seasonally Adjusted," Bureau of Labor Statistics, July 8, 2015, accessed April 21, 2016, www.bls.gov/webapps/legacy/cpsatab14.htm.

[65] Unemployment Rate, Bureau of Labor Statistics, accessed May 15, 2016, http://data.bls.gov/timeseries/LNS14000000.

[66] Nager and Atkinson.

[67] Ibid.; Brian Warmoth, "Immigration and H1B Salaries: Which Tech Companies Pay Most?" DC Inno, March 30, 2016, accessed April 21, 2016, http://dcinno.streetwise.co/2016/03/30/immigration-h-1b-salaries-which-tech-companies-pay-most/.

[68] Nager and Atkinson, citing "Current Population Survey (Median Weekly Earnings of Full-time Wage and Salary Workers by Detailed Occupation and Sex, Household Data Annual Averages)," Bureau of Labor Statistics, accessed March 30, 2015, www.bls.gov/cps/cpsaat39.htm.

[69] Nager and Atkinson, citing "Bachelor's, Master's, and Doctor's Degrees Conferred by Postsecondary Institutions, by Field of Study: Selected years, 1970-71 through 2012-13," National Center for Educational Statistics, 2014 Digest of Education Statistics, accessed March 30, 2015, http://nces.ed.gov/datalab/tableslibrary/viewtable.aspx?tableid=8856.

[70] Nager and Atkinson, citing "Appendix Table 2-19," National Science Foundation, Science and Engineering Indicators 2012, Higher Education in Science and Engineering, accessed March 22, 2015, www.nsf.gov/statistics/seind12/c2/c2s2.htm.

[71] Nager and Atkinson.

[72] Ellen Nakashima, "Federal Agencies, Private Firms Fiercely Compete in Hiring Cyber Experts," *Washington Post*, November 13, 2012, accessed May 16, 2016, https://www.washingtonpost.com/world/national-

security/federal-agencies-private-firms-fiercely-compete-in-hiring-cyber-experts/2012/11/12/a1fb1806-2504-11e2-ba29-238a6ac36a08_story.html.

[73] Gerry Smith and Jeffrey Young, "Uncle Sam Wants Coders to Leave Silicon Valley for DC," Huffington Post, June 11, 2014, accessed April 17, 2016, www.huffingtonpost.com/2014/06/11/washington-tech_n_5475316.html.

[74] Frequently Asked Questions, "Do I Have To Be a Citizen to Apply?" Office of Personnel Management, accessed May 16, 2016, www.opm.gov/faqs/QA.aspx?fid=de14aff4-4f77-4e17-afaa-fa109430fc7b&pid=acfb91ff-c4aa-4b34-b159-7d40c6b45c15; https://www.cia.gov/careers/faq#; https://www.intelligencecareers.gov/nsafaq.html.

[75] Downes and Mayo, 15.

[76] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper," Cisco, February 3, 2016, accessed May 16, 2016, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[77] "Trends in Telecommunication Reform 2016," International Telecommunication Union, 2016, 90-91, accessed May 16, 2016, www.wftp3.itu.int/pub/epub_shared/BDT/2016/2016-Trends/flipviewerxpress.html.

[78] Ibid.

[79] "United States Information Technology Report," BMI Research, 1st quarter 2016, executive summary, accessed May 16, 2016, http://store.bmiresearch.com/united-states-information-technology-report.html.

[80] Ibid.

[81] Mike Freeman, "Sharing Information is the Key to Halting Cyberattacks—Former Homeland Security Chief Tom Ridge Speaks at Cybersecurity Conference," *San Diego Union-Tribune*, October 9, 2015, accessed May 14, 2016, www.sandiegouniontribune.com/news/2015/oct/08/cyber-security-tom-ridge-cyberfest-target-opm

[82] "United States Information Technology Report," BMI Research, 1st quarter 2016, executive summary. Europe in particular took action to relook where and how they share their citizens' data with U.S. companies, ultimately deciding to invalidate the previous Safe Harbor framework. Two years of negotiations with the European Commission did finally result in a new agreement, the EU-U.S. Privacy Shield, which imposes stronger data protection obligations on U.S. ICT companies. The interim period between agreements, however, was fraught with challenges and problems for U.S. businesses until the new agreement was finalized on February 2, 2016. David Faulkner, "Infrastructure for New Smart Sustainable Cities," ITU News, November/December 2015, accessed May 16, 2016, https://itunews.itu.int/En/6274-Infrastructure-for-new-smart-sustainable-cities.note.aspx.

[83] "Internet of Things—Privacy and Security in a Connected World," Federal Trade Commission, January 27, 2015, accessed May 14, 2016, www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[84] *OECD Digital Economy Outlook 2015*," (Paris: OECD Publishing, 2015), 39, accessed May 16, 2016, http://dx.doi.org/10.1787/9789264232440-en.

[85] Ibid.

[86] Bill Goodwin. "Countries Underestimate Risk of Cyber Attack, Says WEF," ComputerWeekly.com, January 15, 2016, accessed May 16, 2016, www.computerweekly.com/news/4500270873/Countries-underestimate-risk-of-cyber-attack-says-WEF.

[87] Press release, "Rep. Ratcliffe Exposes National Security Implications of Cyber Threats." Congressman John Ratcliffe, February 25, 2016, accessed May 10, 2016, https://ratcliffe.house.gov/media-center/press-releases/rep-ratcliffe-exposes-national-security-implications-cyber-threats.

[88] *Science and Engineering Indicators 2016* (Arlington, VA: National Science Foundation, 2016), 4-4, accessed May 16, 2016, www.nsf.gov/statistics/2016/nsb20161/#/report.

[89] Andrew Clevenger, "Defense Department's Budget Requests Seeks More for R&D, ISIS Fight," Defense News, February 9, 2016, accessed May 16, 2016, www.defensenews.com/story/defense/policy-budget/budget/2016/02/09/defense-departments-budget-request-seeks-more-rd-isis-fight/80030752/.

[90] Ashton Carter, "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," U.S. Department of Defense, April 23, 2015, accessed May 16, 2016, www.defense.gov/News/Speeches/Speech-View/Article/606666.

[91] Ibid.

[92] *Revisiting the STEM Workforce, A Companion to Science and Engineering Indicators 2014* (Arlington, VA: National Science Foundation, 2015), accessed April 12, 2016, www.nsf.gov/pubs/2015/nsb201510/nsb201510.pdf.

[93] Kevin Shih, "Labor Market Openness, H-1B Visa Policy, and the Scale of International Student Enrollment in the United States," *Economic Inquiry* 54, no. 1 (January 2016): 122, accessed April 13, 2016, http://onlinelibrary.wiley.com/doi/10.1111/ecin.12250/epdf.

[94] Matt Murphy, "Cyberwar, War in the Fifth Domain," *Economist*, July 1, 2010, accessed May 10, 2016, www.economist.com/node/16478792.

[95] Allison Bender, "Cybersecurity Information Sharing Is Here To Stay," Privacy Tracker, April 3, 2016, accessed April 10, 2016, https://iapp.org/news/a/cybersecurity-information-sharing-is-here-to-stay/.

[96] Aisha Chowdhry, "Despite Pentagon Outreach, Small Tech Firms Say Military Contracting Poses Big Challenges," FCW, April 20, 2016, accessed May 14, 2016, https://fcw.com/articles/2016/04/20/tech-startups-pentagon.aspx.

[97] Jason Tama, "There's No App for That: Disrupting the Military-Industrial Complex," Brookings Institution, July 2015, 2, accessed May 16, 2016, http://www.brookings.edu/research/papers/2015/07/08-military-industrial-complex-silicon-valley-tama.

[98] Chowdhry.

[99] Jack Moore, "White House Wants To Give Agencies New Pot of Money To Upgrade Legacy IT," Nextgov.com, February 9, 2016, accessed May 14, 2016, http://www.nextgov.com/cio-briefing/2016/02/white-house-wants-give-agencies-new-pot-money-upgrade-aging-it/125788/.

[100] Fran Howarth, "What Are the Risks of Legacy Infrastructure?" Security Intelligence, November 24, 2015, accessed May 14, 2016, https://securityintelligence.com/what-are-the-risks-of-legacy-infrastructure/.

[101] Will Goodman, "Lowest Price Technically Acceptable: Overrated, Overused?" *Defense AT&L* 44, no. 2 (March-April 2015): 16-18.

[102] "Proposal Evaluation," Defense Acquisition University ACQuipedia, accessed May 14, 2016, https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=8bdf174c-3b3e-416e-b640-d7091478a5ce.

[103] *Defense Contracting: Factors DoD Considers When Choosing Best Value Processes Are Consistent with Guidance for Selected Acquisitions* (GAO Report No. 14-584) (Washington, DC: Government Accountability Office: July 2014), summary.

[104] *See e.g.*, "Creating Effective Cloud Computing Contracts or the Federal Government: Best Practices for Acquiring IT as a Service," CIO Council and Chief Acquisition Officers Council, February 24, 2012, accessed May 14, 2016, https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

[105] *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, (CRS Report No. R42887) (Washington, DC: Congressional Research Service, January 20, 2015).

[106] *High Risk Series: An Update*, (GAO Report No. GAO-15-290) (Washington, DC: Government Accountability Office, February 2015), 37-54; "Cloud Adoption Among Government Entities to Skyrocket, Says Report by Forbes Insight and Microsoft," Forbes, May 21, 2015, accessed May 14, 2016, www.forbes.com/sites/forbespr/2015/05/21/cloud-adoption-among-government-entities-to-skyrocket-says-report-by-forbes-insights-and-microsoft/#2e47e0ff3a29.

[107] Peter Swire, "The Government Shouldn't Weaken Encryption. We're Already in a Golden Age of Surveillance," Slate, July 15, 2015, accessed April 16, 2016, www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

[108] Declan McCullagh, "Surveillance 'Partnership' Between NSA and Telcos Points to AT&T, Verizon," CNET, June 27, 2013, accessed April 16, 2016, www.cnet.com/news/surveillance-partnership-between-nsa-and-telcos-points-to-at-t-verizon/.

[109] *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, Motion to Compel, Case No. CM 16-10 (C.D. Cal., February 19, 2016), accessed May 16, 2016, www.justice.gov/usao-cdca/file/826836/download.

[110] "What is TOR?" TOR, accessed May 14, 2016, www.torproject.org.

[111] "Don't Panic, Making Progress on the 'Going Dark' Debate," Berkman Center for Internet & Society at Harvard University, 5, accessed May 16, 2016, https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[112] "Clipper Chip," Cryptomuseum.com, accessed May 14, 2016, www.cryptomuseum.com/crypto/usa/clipper.htm.

[113] "Don't Panic, Making Progress on the 'Going Dark' Debate."

[114] Mary Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center, November 12, 2014, accessed May 14, 2016, www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[115] Yochai Benkler, "We Cannot Trust Our Government, So We Must Trust the Technology," *Guardian*, February 22, 2016, accessed April 16, 2016, www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

[116] Ibid.

[117] David Curry, "Microsoft Announces Local Data Centers for German Cloud Users to Avoid U.S. Spies," Digital Trends, November 11, 2015, accessed May 14, 2016, www.digitaltrends.com/computing/microsoft-german-data-centers/; Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times*, March 21, 2014, accessed May 14, 2016, www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0.

[118] Spencer Ackerman, "Lavabit Email Service Abruptly Shut down Citing Government Interference," *Guardian*, August 09, 2013, accessed April 20, 2016, www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden.

[119] Michael Friberg, "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," Wired, April 5, 2016, accessed May 14, 2016, www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

[120] "Decrypting an IPhone for the FBI," Schneier on Security, February 22, 2016, accessed April 16, 2016, www.schneier.com/blog/archives/2016/02/decrypting_an_i.html; Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," July 7, 2015, accessed April 16, 2016, www.schneier.com/cryptography/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

[121] "Don't Panic, Making Progress on the "Going Dark" Debate." Appendix A.

[122] Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013, accessed April 20, 2016, www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[123] "Decoding the Encryption Dilemma: A Conversation on Backdoors, Going Dark, and Cybersecurity," Information Technology and Innovation Foundation, March 31, 201, accessed April 20, 2016, https://itif.org/events/2016/03/31/decoding-encryption-dilemma-conversation-backdoors-going-dark-and-cybersecurity.

[124] Not all data will be encrypted, especially as companies seek to retain some of the targeted revenue raising methods that depend on an ability to know something about the user, and as the Internet of Things rapidly expands.

[125] Peter Mell, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, April 27, 2012, accessed April 10, 2016, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[126] Ibid.

[127] Ibid.

[128] Ibid.

[129] Ibid.

[130] Ibid.

[131] "Global Cloud Computing Service Market Expects to Reach $555 Billion Worth by 2020," Business 2 Community, July 31, 2014, accessed April 10, 2016, www.business2community.com/cloud-computing/global-cloud-computing-service-market-expects-reach-555-billion-worth-2020-0961446#6u9sCttPJ9pCSbp7.97.

[132] Gavin Clarke, "Oracle Salesmen Get SEVENFOLD Salary Boost for Flogging Its Cloudy AaS Produce," The Register, March 19, 2015, accessed April 10, 2016, www.theregister.co.uk/2015/03/19/oracle_cloud_sales_staff_sevenfold_bonus_selling_aas/.

[133] Matt Rosoff, "Microsoft Vows to Have $20 Billion in Cloud Revenue in 2018," Business Insider, April 29, 2015, accessed April 10, 2016, www.businessinsider.com/microsoft-20-billion-cloud-revenue-and-1-billion-windows-10-pcs-by-2018-2015-4.

[134] Bernard Golden. "Amazon Opens up about AWS Revenues," CIO, May 12, 2015, accessed April 10, 2016, www.cio.com/article/2921180/cloud-computing/amazon-opens-up-about-aws-revenues.html.

[135] Molly Walker, "Report: Government Increases Cloud Spending," *FierceGovernmentIT*, February 17, 2016, accessed May 16, 2016, www.fiercegovernmentit.com/story/report-government-increases-cloud-spending/2016-02-17.

[136] "Program Overview," Fed RAMP, accessed May 16, 2016, www.fedramp.gov/.

[137] Ibid.

[138] Ibid.

[139] Gerry Connell, "Congressional Cloud Computing Caucus Inaugural Report Provides Metrics and Insight on the State of Federal Cloud Computing Progress," Business Wire, May 11, 2015, accessed May 16, 2016, www.businesswire.com/news/home/20150511006195/en/Congressional-Cloud-Computing-Caucus-Inaugural-Report-Metrics.

[140] Ibid.

[141] Ibid

[142] "Advanced Wireless Services," Federal Communications Commission, accessed April 17, 2016, http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=97.

[143] "Regulating the Use of Spectrum," National Telecommunications and Information Administration, accessed April 9, 2016, www.ntia.doc.gov/book-page/regulating-use-spectrum.

[144] "The Value of Mobile Services," GSMA, accessed April 15, 2016, www.gsma.com/spectrum/the-value-of-mobile/.

[145] Public Law 73-416, 48 Stat. 1064, June 19, 1934.

[146] Public Law 108-494, 118 Stat. 3991, December 23, 2004.

[147] Regulating the Use of Spectrum," National Telecommunications and Information Administration.

[148] Ibid.

[149] Randolph J. May, The Free State Foundation, "Response to Questions in the Second White Paper," before the U.S. House of Representatives Committee on Energy and Commerce, April 24, 2014, accessed May 16, 2016, www.freestatefoundation.org/images/Response_to_Questions_in_the_Second_White_Paper_042414.pdf.

[150] Ibid.

[151] *Dynamic Spectrum Management* (Wilmington, DE: InterDigital, October 2012), accessed May 16, 2016, www.interdigital.com/download/54313edbe26228452500022c.

[152] Ibid.

[153] Jeff Swiatek, "H-1B Visa Is a Hot Ticket for Tech Workers in Central Indiana," IndyStar, May 1, 2014, accessed May 14, 2016, www.indystar.com/story/money/2014/04/19/h-b-visa-hot-ticket-tech-workers-central-indiana/7887513/.

[154] "National Broadband Plan," Federal Communications Commission, March 17, 2010, accessed May 14, 2016, www.fcc.gov/general/national-broadband-plan.

[155] Klaus Schwab, *The Global Competitiveness Report 2015-2016* (Geneva: World Economic Forum, 2015), 361, accessed April 21, 2016, www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf.

[156] Ibid.

[157] *2016 Broadband Progress Report*, Federal Communications Commission, Docket No. 15-191, January 29, 2016, accessed April 21, 2016, www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

[158] *2016 Broadband Progress Report*, xiv.

[159] Larry Downes, "Did the National Broadband Plan Spur Innovation?" *Washington Post*, March 23, 2015, accessed May 16, 2016, www.washingtonpost.com/news/innovations/wp/2015/03/23/did-the-national-broadband-plan-spur-innovation/.

[160] *The State of the Art and Evolution of Cable Television and Broadband Technology* (Kensington, MD: CTC Technology & Energy, October 9, 2013), 7, accessed April 21, 2016, http://ctcnet.us/SeattleCATVTechnologyReport.pdf.

[161] Jon Brodkin, "Verizon Nears 'the end' of FiOS Builds," *ARS Technica*, January 23, 2015, accessed April 21, 2016, http://arstechnica.com/business/2015/01/verizon-nears-the-end-of-fios-builds/.

[162] "Fiber-Optic Internet in the United States," *BroadbandNow*, accessed April 21, 2016, http://broadbandnow.com/Fiber.

[163] Larry Downes, "Race to Gigabit Internet Service Takes Off," *CNET*, August 31, 2004, accessed April 21, 2016, www.cnet.com/news/race-to-gigabit-internet-service-takes-off/.

[164] *Connecting America: The National Broadband Plan*, Federal Communications Commission, March 17, 2010, xi, accessed April 21, 2106, https://transition.fcc.gov/national-broadband-plan/national-broadband-plan-executive-summary.pdf.

[165] "Mobile Wireless Internet in the United States," *BroadbandNow*, accessed April 21, 2016, http://broadbandnow.com/Mobile.

[166] Klaus Schwab, "The Global Competitiveness Report 2015-2016."

[167] "State of Mobile Networks: USA," OpenSignal, February 2016, accessed April 21, 2016, https://opensignal.com/reports/2016/02/usa/state-of-the-mobile-network.

[168] Ibid.

[169] Larry Downes, "Take Note Republicans and Democrats, This Is What a Pro-innovation Platform Looks Like," *Washington Post*, January 7, 2015, accessed April 21, 2016, www.washingtonpost.com/news/innovations/wp/2015/01/07/take-note-republicans-and-democrats-this-is-what-a-pro-innovation-platform-looks-like/.

[170] *In the Matter of Protecting & Promoting the Open Internet*, 30 F.C.C. Rcd 5601 (2015).

[171] Mark Cooper, "The Long History and Increasing Importance of Public-Service Principles for 21st Century Public Digital Communications Networks," *Journal n Telecommunications & High Technology Law* 12 (2014): 6.

[172] Ibid.

[173] *In the Matter of Preserving the Open Internet*, 25 F.C.C. Rcd 17905, para. 32 (2010), vacated and remanded by *Verizon v. FCC*, 740 F.3d 623 (DC Cir. 2014).

[174] Jon Brodkin, "One Big Reason We Lack Internet Competition: Starting an ISP is Really Hard," Ars Technica, April 6, 2014, accessed April 21, 2016, http://arstechnica.com/business/2014/04/one-big-reason-we-lack-internet-competition-starting-an-isp-is-really-hard/; Gene Kimmelman and Mark Cooper, "Antitrust and Economic Regulation: Essential and Complementary Tools to Maximize Consumer Welfare and Freedom of Expression in the

Digital Age," *Harvard Law & Policy Review* 9 (2015): 407-08, citing Alfred E. Kahn, *The Economics of Regulation: Principles and Institutions* Vol. I (Cambridge: MIT Press, 1988): 11.

[175] Elise A Couper, John P. Hejkal, and Alexander L. Wolman, "Boom and Bust in Telecommunications," Federal Reserve Bank of Richmond, *Reserve Quarterly* 89, no. 4 (Fall 2003).

[176] Kimmelman and Cooper, 436.

[177] Robert E. Litan and Hal J. Singer, "Why Business Should Oppose Net Neutrality," *Harvard Business Review*, August 13, 2010, accessed April 20, 2016, https://hbr.org/2010/08/why-business-should-oppose-net-neutrality.

[178] *In the Matter of Protecting & Promoting the Open Internet*, para. 2.

[179] Robert Cannon, "The Legacy of the Federal Communications Commission's Computer Inquiries," *Federal Communications Law Journal* 55 (2003): 174.