NISKANEN CENTER

Public Interest Comment

Submitted to the National Telecommunications Information Administration in the Matter of:

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Ryan Hagemann

Technology and Civil Liberties Policy Analyst
The Niskanen Center

Submitted: May 23, 2016
Docket No. 160331306-6306-01

Executive Summary

The Internet of Things (IoT) is an emerging ecosystem of technologies and digital networks that will soon become a driver of economic growth. The IoT will likely disrupt incumbent industries, but these changes on the whole will benefit consumers and producers alike. Issues requiring the attention of regulators, policymakers, and industry stakeholders are sure to arise. This comment offers an intellectual framework for addressing those issues.

A hands-off regulatory approach to the Internet helped catalyze the growth of the modern digital economy. The government should approach the IoT in the same way. In order to foster the advancement of the IoT, the Niskanen Center recommends that the federal government (1) embrace a regulatory framework similar to that of the one promoted by the Clinton Administration for the emerging Internet, and (2) abstain from non-Congressional bureaucratic processes or stakeholder engagements that might negatively impact the pace of innovation in this space.

Introduction

The Internet of Things (IoT) is a burgeoning area of technological development. Its ascent promises significant economic benefits, in part through the "disruption" of existing technologies on a scale similar to, and possibly superseding, the emergence of the commercial Internet in the early 1990s. Some industry analysts forecast that the number of devices connected to the Internet, and therefore part of the IoT, will number in the tens of billions, and may even approach one trillion, with potential economic gains projected to range from $2.7 to 6.2 trillion *annually* by 2025.[1] Other analysts have placed the potential benefits as high as $19 trillion.[2] As the price of remote frequency identification (RFID) chips and micro-electromechanical systems (MEMS) continue to fall, sensor-equipped components are likely to become embedded in even the most common everyday objects.

The impending proliferation of embedded sensors leaves puts the IoT in a position to reconfigure whole sectors of the economy. Samuel Greengard, author of *The Internet of Things*, writes:

> *The Internet of Things will introduce new products and services and make many existing offerings completely obsolete. The technology will eliminate jobs but introduce new lines of work. Connected systems will ripple through education, government, and business and fundamentally remap and rewire actions, behavior, and social norms. The technology will affect everything from the way people vote to the way we eat at restaurants and take vacations.*[3]

Rapid, potentially revolutionary change inevitably creates anxiety. Some people are skittish about a more ubiquitously interconnected world, and many of their worries are entirely reasonable.[4] In particular, fears that the the IoT may threaten privacy and enable surveillance are worth taking very seriously. But these concerns should not blind us to the potential benefits of the IoT. Many of the same concerns were raised during the development of the Internet. Nevertheless, the Internet has become an immensely valuable tool and resource for people the world over. It's important to address concerns about and potential costs of the IoT without sidelining its development, lest we lose out on its many promising benefits.

We are grateful for the opportunity to respond to NTIA's questions regarding the IoT. Given the many questions to which NTIA has requested answers, we have attempted to answer only those regarding matters on which which the Niskanen Center has expertise. Our comments will focus specifically on general issues (questions 1-3), economic issues (question 13), policy issues (questions 15-17), and additional issues (questions 25-27). For ease of navigation, the original

---

[1] "Disruptive Technologies: Advances that will transform life, business, and the global economy," *McKinsey Global Institute*, May 2013, p. 51, http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies.

[2] "The Internet of Everything—A $19 Trillion Opportunity," Cisco Consulting Services, http://www.cisco.com/c/dam/en_us/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf.

[3] Samuel Greengard, "The Internet of Things," The MIT Press (Cambridge, MA), 2015, p. Xv.

[4] Andy Meek, "What Role should the government play in developing the internet of things?, *The Guardian*, October 14, 2015, https://www.theguardian.com/technology/2015/oct/14/government-regulation-internet-of-things.

questions promulgated by NTIA have been included for reference. In addition to footnote citations, a copy of the original text of the "Framework for Global Electronic Commerce" that is cited throughout these comments has been included after the "Conclusion" section.

General Questions

Question 1: *Are the challenges and opportunities arising from ioT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?*

a. *What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?*
b. *What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?*
c. *What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?*

In the late 1980s and early 1990s, there were many concerns about the possible implications of the emerging Internet. Many of the concerns about the IoT are similar to, if not the same as, those about the early Internet. The Clinton Administration wisely abstained from imposing *ex ante* regulations on the Internet. As a result, the Internet was able to evolve and mature according to the needs, demands, and concerns of innovators and entrepreneurs, consumers, and a wide array of other stakeholders. The same principles that informed the approach to regulating the Internet should also inform policymakers' and regulators' perspectives on the emerging IoT. Those principles are contained within the accompanying "Framework for Global Electronic Commerce," and would serve as an ideal frame of reference for how best to approach regulation and standard-setting for the IoT.[5]

Question 2: *The term "Internet of Things" and related concepts have been defined by multiple organizations, including parts of the U.S. government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?*

The problem with attempting to define the IoT in any specific, narrowly-tailored manner is that it is likely to fail to capture the breadth of the emerging technological ecosystem. Whether we call it the "Internet of Things," the "Internet of Living Things," or something else, the essence of the emerging phenomenon is best captured by the "Internet of *Everything*." Definitions that precede a fuller development of the technology may be of limited use.

Still, it's important to limit the scope of the domain. The best definition of the IoT so far comes from the Internet Society:

> *The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday*

[5] "Framework for Global Electronic Commerce," July 1, 1997, https://www.w3.org/TR/NOTE-framework-970706. (Also included after the "Conclusion" section of these comments for reference)

items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.

However, the Internet Society goes on to say that there is "no single, universal definition" of the IoT.[6] Although the Federal Trade Commission's (FTC) definition is similar, it specifies that the devices in question are "designed for businesses," which fails to capture the true breadth of the IoT landscape.[7]

Question 3: *With respect to current or planned laws, regulations, and/or policies that apply to IoT:*

a. *Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?*
b. *Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?*

Congress is currently considering the Developing Innovation and Growing the Internet of Things (DIGIT) Act. This legislation would convene a working group "of Federal stakeholders to provide recommendations to Congress on how to appropriately plan for and encourage the proliferation of the Internet of Things in the United States."[8] Such a working group would likely foster the development of the IoT, and address many of the policy questions in NTIA's request for comments. The Niskanen Center supports the DIGIT Act as a necessary first step towards establishing a national strategy on IoT that will ensure the United States remains the preeminent leader in its development. In a statement of support for the DIGIT Act, Daniel Castro, Vice President of the Information Technology and Innovation Foundation, noted:

> *The success of the Internet today can be traced back to smart public policies that proactively supported the growth of the technology. It is encouraging to see policymakers taking the opportunity to repeat this successful approach for the Internet of Things. The DIGIT Act will bring together a broad cross section of stakeholders in government and industry to shape policies on the Internet of Things, ensuring that the United States can successfully capture the wide variety of benefits it has to offer in both the public and private sectors.*[9]

---

[6] "The Internet of Things: An Overview," *The Internet Society*, October 2015, pp. 16-17, http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf.

[7] In particular, the FTC defines the IoT to include devices, products, and services "designed for businesses to enable automated communications between machines … things such as devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet." While the FTC is certainly tailoring its definition to focus on its mandate vis-a-vis consumer protection from egregiously deceptive and unfair business practices, the implications of the IoT go well beyond commercial applications. Thus, the agency's definition is lacking for the purposes of NTIA's question. Internet

[8] "Developing Innovation and Growing the Internet of Things Act," Section 3(b)(1), http://www.fischer.senate.gov/public/_cache/files/03de7771-088b-45ac-8552-f82ddc0aa480/digit-2016---final-bill-for-filing.pdf.

[9] "Bipartisan DIGIT Act Could Make US the Global Leader on the Internet of Things," *Information Technology and Innovation Foundation*, March 1, 2016, https://itif.org/publications/2016/03/01/bipartisan-digit-act-could-make-us-global-leader-internet-things.

The Niskanen Center concurs. We believe that the DIGIT Act will be useful in realizing the benefits of the IoT.

Economic Issues

Question 13: *What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?*

a. *What will be the benefits, if any?*
b. *What will be the challenges, if any?*
c. *What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?*

The McKinsey Global Institute estimates that the IoT will have a greater economic impact on manufacturing than on any other sector of the economy. By 2025, this impact has "the potential to create value of $1.2 trillion to $3.7 trillion."[10] These economic gains will come from increased collection, analysis, and use of data from embedded and networked RFID and MEMS sensors, which will create many new efficiencies in a number of areas including: monitoring and control of production tools; automation of quality control; maintenance of capital machinery; workfloor safety, through preemptively alerting individuals to hazardous situations; optimization of production and supply-chain flows; and automated self-adjustment of equipment in response to changes in conditions (e.g. change in the type of production occurring). Productivity could be increased by as much as 10 to 25 percent, leading to savings approaching $1.8 trillion annually. Additionally, there may be very large gains from reductions in the cost of production, predictive maintenance, and increased health and safety, to name but a few of the many possible benefits.[11]

In short, the implications of IoT for manufacturers are immense. As the McKinsey Global Institute report goes on to note:

> *Use of IoT in the factory setting has the potential to alter the relationships among manufacturers, distributors, consumers, and lenders. For manufacturers, IoT-based systems have the potential not only to improve the performance at individual plants, but also to help provide greater visibility into performance throughout production facilities, allowing manufacturers to optimize production across locations and situations. These productivity improvement could be used to build up scale and improve profitability.*[12]

Every step of the manufacturing process, from production to distribution, will move towards greater optimization as a result of the IoT. Producers will see reduced costs—and increased profitability. Consumers will enjoy lower prices. Optimizing logistical supply lines will allow savings on everything from labor costs to fuel consumption in the distribution of goods. As producers converge on these cost-cutting measures, they will

[10] James Manyika, et. al., "The Internet of Things: Mapping the Value Beyond the Hype," *McKinsey Global Institute*, June 2015, p. 66.
[11] Ibid. pp. 66-74.
[12] Ibid. p. 73.

be driven to seek competitive advantages in data analytics, spurring further innovation and demand for the services of software engineers, data analysts, and technical repairmen.

Of course, the benefits don't end at manufacturing or industrial-scale efficiencies. Sectors such as health care, urban infrastructure, resource extraction, retail, and others stand to benefit on a scale ranging from tens to hundreds of billions of dollars in economic gains by 2025. Industrial manufacturing stands to gain the lion's share of these benefits in the first wave of the IoT revolution, but that is just the peak of the iceberg.

Policy Issues

Question 15: *What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?*

The primary policy issues raised by the IoT include privacy, cybersecurity, law enforcement issues, and consumer protection more broadly.

The policy landscape of the IoT very closely mirrors that of the Internet. Issues such as privacy and cybersecurity primarily dominate the headlines, but this could change as the IoT evolves and more products and services enter the market. Regulators and policymakers should recognize the limits of their knowledge and act with humility, forbearing from attempting to address problems using top-down, heavy-handed regulation. The government can best address these concerns by relying on existing rules and agency authority. FTC Commissioner Maureen Ohlhausen rightly maintains that the FTC can play a valuable role:

> *The FTC's approach of doing policy R&D to get a good understanding of the [IoT], educating consumers and businesses about how to maximize its benefits and reduce its risks, and using our traditional enforcement tools to challenge any harms that do arise offers, in my opinion, the best approach. This type of informed action will allow free markets and technological innovation to serve the greatest good, while still maintaining a federal role in protecting consumers and ensuring a level playing field for competitors.*[13]

It is important to ensure "a level playing field" with respect to IoT innovation. However, as Ohlhausen notes, "free markets and technological innovation" are the primary mechanisms by which the benefits of the IoT will be realized. The FTC, NTIA, and other federal agencies must recognize that they cannot possibly predict or plan for all the pitfalls that may arise as this technology matures. They can, however, prevent many benefits of the IoT from materializing by regulating too early or in too heavy-handed a manner. The risk of premature and excessive regulation is especially acute given the size of the potential economic benefits to American producers and consumers.

---

[13] "The Internet of Things: When Things Talk Among Themselves," Remarks of Commissioner Maureen K. Ohlhausen FTC, Internet of Things Workshop, November 19, 2013, https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf.

Question 16: *How should the government address or respond to cybersecurity concerns about IoT?*

a. *What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?*
b. *How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?*
c. *What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?*

The government can play a positive role in addressing cybersecurity, but needs to get its own house in order. Over the past year, several government agencies have been hacked. This shows how important proper cybersecurity practices are in securing networks, and also how inadequate the government's standards and responses have been. Until the government steps up and shows itself to be a competent cybersecurity practitioner, it may be difficult to promulgate rules and regulations that achieve the level of private-sector buy-in needed to make them truly effective. If the government finds its own standards too difficult to implement effectively, it can't expect industry to take its recommendations on cybersecurity entirely seriously. For now, the government should permit industry to self-regulate, which it has every incentive to do well.

Self-regulating mechanisms, such as industry-based standards, can serve producers and consumers well in this space, and better than standards that might be issued by government. The Online Trust Alliance's (OTA) Trust Framework serves as a good example of how industry self-regulation can anticipate the need for addressing potential problems before they arise. Its emphasis on "security and privacy by design" illustrates the priorities of companies operating in the IoT space.[14] These types of industry-led standards should be permitted to set the agenda in cybersecurity regulation. When market failures can be demonstrated, and demonstrated to require government intervention, then and only then should the government address the issue through legislation or regulation.

The most effective tool for addressing cybersecurity concerns is strong encryption. Therefore, the Department of Commerce (DOC), and NTIA in particular, should promote the use of encryption in IoT services and products as a core policy prescription for dealing with security issues raised by ubiquitous interconnectivity of networked devices. Cybersecurity is vital for a modern digital economy. Strong encryption has massive economic benefits, produced in large measure by encouraging and promoting the trust necessary for a flourishing ecosystem of online commerce and finance.[15] The economic benefits of the security and trust that strong encryption provides should be expected to transfer over to the IoT ecosystem.

Question 17: *How should the government address or respond to privacy concerns about IoT?*

---

[14] "IoT Trust Framework," Online Trust Alliance, https://otalliance.org/IoT.

[15] Ryan Hagemann and Joshua Hampson, "Encryption, Trust, and the Online Economy: An Assessment of the Economic Benefits Associated with Encryption," *Niskanen Center*, November 9, 2015, https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?
b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?
c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

Privacy is an amorphous concept without a single uncontested meaning.[16] The possibility that governments may tap into IoT networks for surveillance purposes raises one set of important concerns. Private sector collection of user data presents a separate set of concerns, which the government is less capable of effectively regulating *ex ante*. The Fourth Amendment and other statutes already legally limit the government's power to invade the privacy of citizens. However, in those cases in which the intelligence community and law enforcement are allowed by the prevailing interpretation of law to evade those limits, the government—and Congress in particular—ought to step in to clarify the law in order to more thoroughly secure the privacy of Americans against unwarranted and "incidental" collection of innocent Americans' data.

As noted by the McKinsey report:

> *Policy makers faced with these issues will need to think comprehensively and globally. One-off regulations and rules that are in conflict from one jurisdiction to another will not suffice. Policy makers will need to build consensus regarding what protection to put in place and work across borders and levels of government to make sure these protections can and will be universally enforced.*[17]

The development of the necessary consensus is already under way with the introduction of the DIGIT Act, previously mentioned. While there is no assurance of its passage, policymakers need to send a clear message in to help achieve market certainty about the future of the IoT. The message should be this: that Congress, and not a confusing hodgepodge of competing regulatory bodies, will be the primary regulator of the IoT. Congress, not executive branch regulators, should lead on the IoT.

The privacy concerns raised by the IoT are fundamentally no different from those raised by the emergence and proliferation of the Internet. If the Internet did not require a structured regulatory response to privacy concerns, neither does the IoT. At this time, a federal approach to setting privacy norms would be premature and could have unintended consequences hampering innovation in the IoT space.[18]

---

[16] Larry Downes, "A Rational Response to the Privacy 'Crisis'," *Cato Institute*, Policy Analysis No. 716, January 7, 2013, http://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

[17] "Disruptive Technologies," p. 60.

[18] One example of how such innovation might have been forestalled is the case of Google's Gmail service. Had the government limited private sector data collection in the infant stages of the Internet's evolving ecosystem, hundreds of millions of people would never have known the benefit of using an ostensibly "free" email service. (Susie Poppick, "10 Ways Google Has Changed the World, *Time*, August 18, 2014, http://time.com/money/3117377/google-10-ways-changed-world/.) As another example, the economic benefits of "Big Data" could have been squelched in their infancy if the government had imposed onerous

Additionally, the FTC is already well-positioned to deal with potential violations of user privacy agreements, as discussed in response to Question 18.

Question 18: *Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?*

As the IoT continues to grow, there are likely to be complications arising from violations of user privacy agreements, as well as situations involving fraud and deceptive practices. But these issues are not fundamentally different from those federal regulators currently address.

Ample authority already exists under FTC's power to prohibit and address unfair and deceptive practices. In particular, the FTC is authorized to police "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[19] The broad statutory power afforded the Commission allows it to sufficiently address consumer harms that may result from breaches of contract between IoT service providers or product manufacturer and consumers. Other policy analysts specializing in the IoT and technology policy have made similar observations.[20]

Additional Issues

Question 25: *Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?*

As an emerging technology, the IoT is likely to spawn many unseen and currently unknown issues that could require the attention of policymakers and industry players. However, experience has shown that multistakeholder processes, though launched with the best of intentions, are seldom the best way to produce timely, effective recommendations. There tend to be too many parties involved and the inherent uncertainty of the process can lead to wariness in market actors. In general, NTIA multistakeholder processes have a tendency to become convoluted and procedurally overbearing unless structured to achieve a very specific objective.[21]

Unless mandated by Congress or the Administration, such processes should be avoided whenever possible. Unless a clear need for a multistakeholder engagement emerges, NTIA should refrain from initiating such a process.

---

regulations surrounding the collection of individuals' data. Instead, pursuant to user privacy agreements, many of these benefits are only beginning to be realized and will likely continue contributing to the evolution of the IoT. ("Big Data: Seizing Opportunities, Preserving Values," *Executive Office of the President*, May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.)

[19] 15 U.S. Code § 45

[20] Adam Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation," *Mercatus Working Paper*, November 2014, http://mercatus.org/sites/default/files/Thierer-Wearable-Tech.pdf.

[21] Berin Szoka, "The Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct," submitted April 12, 2012, http://docs.techfreedom.org/Comments_NTIA_Multistakeholder_4.12.12.pdf.

Question 26: *What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters?*

See response to Question 25.

Question 27: *How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?*

A clear and settled government approach to the IoT would create market certainty and, if tailored appropriately to industry needs, help maximize the potential social and economic benefits of this emerging technology. However, the approach would need to embody regulatory humility as a guiding practice for federal agencies. Otherwise, onerous regulations could curtail innovation in the IoT. As the Information Technology and Innovation Foundation's Center for Data Innovation discussed in a recent paper on this topic:

> *Creating restrictive rules for an emerging technology at such an early stage in its development without clear evidence of concrete consumer harms can have the unintended consequence of limiting innovation by unnecessarily hampering certain business models or raising costs. Moreover, the privacy fears associated with new technologies are often substantially inflated.*
>
> *A national strategy for the Internet of Things can forestall such problems by sending a clear message to legislators and regulators that this technology is important and that over-regulation or poorly-designed regulation would limit its growth. Moreover, a national strategy can encourage legislators and regulators to focus on regulations that would expand, rather than limit use of the Internet of Things.*[22]

As noted in the response to Question 3, the DIGIT Act serves as a good starting point for fleshing out many of the concerns NTIA's comments seek to address. Since Congress has already begun taking a legislative lead on the IoT, deference should be given to the conclusions of the working group established by the DIGIT Act, which would include DOC and NTIA as major stakeholders in the working group structure.

General Policy Recommendations

A long list of detailed recommendations could be provided. However, at this early stage in the development of the IoT, it is more useful to set out general principles to guide policymaking going forward. To that end, the following two recommendations should serve as guidance for the DOC, NTIA, and other federal agencies examining possible action on the IoT.

[22] Joshua New and Daniel Castro, "Why Countries Need National Strategies for the Internet of Things," *ITIF, Center for Data Innovation*, December 16, 2015, P. 9, http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

Recommendation #1: The tenets of the "Framework for Global Electronic Commerce" should guide the federal government's approach to regulating the IoT.

The Clinton Administration's "Framework for Global Electronic Commerce," which provided a clear roadmap for how and when the federal government should intervene in the development of the Internet, is as relevant today as it was in the mid-1990s.

The IoT is simply the next stage in the evolution of the Internet. That fact should be reflected in the government's acceptance and continued application of this framework, which helped transform the Internet into the global platform for innovation, creativity, and economic growth that it is today. A similarly relaxed policy towards the IoT can do wonders for its ongoing maturation, while providing the market certainty necessary to continue to promote investment, innovation, and research and development.

In particular, the first four principles laid out in that framework can just as easily apply to the emergence of the IoT. Substituting "IoT" for instances of "the Internet" throughout the first four principles yields suggestions that are wholly consistent with an approach that embraces the same regulatory forbearance and recognition of the value of market forces in driving innovation. As such, the framework could be adapted to the IoT to read along the following lines:

1. **"The private sector should lead."** The framework specifies that "governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the" IoT. "Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them."
2. **"Governments should avoid undue restrictions" on the IoT.** "Unnecessary regulation of commercial activities will distort development of the electronic marketplace by decreasing the supply and raising the cost of products and services for consumers. … [G]overnment attempts to regulate are likely to be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific. Accordingly, governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the" IoT.
3. **"Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."** The framework specifies that "where government intervention is necessary to facilitate" the development of the IoT, "its goal should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution."
4. **"Governments should recognize the unique qualities of the" IoT.** "Regulation should be imposed only as a necessary means to achieve an important goal on which there is broad consensus. Existing laws and regulations that may hinder electronic commerce [and the continued development of the IoT] should be reviewed and revised or eliminated to reflect the needs of the new electronic age."[23]

[23] "Framework for Global Electronic Commerce."

By adhering to the essential language of these four principles, the government can most effectively contribute to the continued development and evolution of the IoT. Doing so will also underscore the fact that the principles that guided the growth of the Internet ecosystem can, and should, be applied wholesale to the IoT, which is little more than the next evolutionary step in the Internet's development.

Recommendation #2: Refrain from IoT-specific mandates, multistakeholder processes, or other efforts that would act as bureaucratic impediments to innovation.

Thus far, the private sector has done a commendable job addressing consumer concerns related to the IoT. Unless a clear and pressing need arises calling for engagement from the DOC, and specifically NTIA, it should remain hands-off. NTIA should clearly communicate that it recognizes the limits of its knowledge about the development of the IoT, and the nature and importance of the concerns that may arise. Furthermore, NTIA should be clear that it understand the limits of its power to effectively address potential harms. The FTC's Section 5 Authority is better equipped to deal with consumer-related abuses than the DOC; as such, NTIA should defer to the FTC's regulatory authority on issues related to consumer harm.

If NTIA chooses, or is mandated by the Administration or Congress, to convene a multistakeholder process to produce best practices, codes of conduct, or other standards, we urge it to tailor clear, transparent rules for how such a process will unfold.[24]

Conclusion

Government can offer valuable assistance to the private-sector by laying down general rules of the game regarding the development and use of new technologies, such as the IoT. However, as with any emerging technology, the federal government should embrace the regulatory equivalent of the Hippocratic Oath: first, do no harm. The speed of technological development long ago outpaced the ability of traditional regulatory agencies to deal with problems in an effective *ex ante* manner. This is especially true in the IoT space. Just as the Clinton Administration embraced a more relaxed regulatory framework for the Internet, so too should current regulators embrace a hands-off approach to the IoT. The Niskanen Center is grateful for the opportunity to comment on issues related to this important, and still-nascent, area of technological development.

[24] For a more detailed perspective on how NTIA could potentially structure such proceedings, we refer the agency to comments submitted by TechFreedom in the matter of "The Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct," submitted April 12, 2012, http://docs.techfreedom.org/Comments_NTIA_Multistakeholder_4.12.12.pdf, as well as TechFreedom's comments in the matter of "Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems," submitted April 20, 2015 https://www.ntia.doc.gov/files/ntia/techfreedom_4.20.15.pdf.

Framework for Global Electronic Commerce

1 July 1997
(Originally accessed at https://www.w3.org/TR/NOTE-framework-970706)

Background

The Global Information Infrastructure (GII), still in the early stages of its development, is already transforming our world. Over the next decade, advances on the GII will affect almost every aspect of daily life -- education, health care, work and leisure activities. Disparate populations, once separated by distance and time, will experience these changes as part of a global community.

No single force embodies our electronic transformation more than the evolving medium known as the Internet. Once a tool reserved for scientific and academic exchange, the Internet has emerged as an appliance of everyday life, accessible from almost every point on the planet. Students across the world are discovering vast treasure troves of data via the World Wide Web. Doctors are utilizing tele-medicine to administer off-site diagnoses to patients in need. Citizens of many nations are finding additional outlets for personal and political expression. The Internet is being used to reinvent government and reshape our lives and our communities in the process. As the Internet empowers citizens and democratizes societies, it is also changing classic business and economic paradigms. New models of commercial interaction are developing as businesses and consumers participate in the electronic marketplace and reap the resultant benefits. Entrepreneurs are able to start new businesses more easily, with smaller up-front investment requirements, by accessing the Internet's worldwide network of customers.
Internet technology is having a profound effect on the global trade in services. World trade involving computer software, entertainment products (motion pictures, videos, games, sound recordings), information services (databases, online newspapers), technical information, product licenses, financial services, and professional services (businesses and technical consulting, accounting, architectural design, legal advice, travel services, etc.) has grown rapidly in the past decade, now accounting for well over $40 billion of U.S. exports alone.

An increasing share of these transactions occurs online. The GII has the potential to revolutionize commerce in these and other areas by dramatically lowering transaction costs and facilitating new types of commercial transactions.

The Internet will also revolutionize retail and direct marketing. Consumers will be able to shop in their homes for a wide variety of products from manufacturers and retailers all over the world. They will be able to view these products on their computers or televisions, access information about the products, visualize the way the products may fit together (constructing a room of

furniture on their screen, for example), and order and pay for their choice, all from their living rooms.

Commerce on the Internet could total tens of billions of dollars by the turn of the century. For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce. Official decision makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining features of the new digital marketplace.

Many businesses and consumers are still wary of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions. This is particularly true for international commercial activity where concerns about enforcement of contracts, liability, intellectual property protection, privacy, security and other matters have caused businesses and consumers to be cautious.

As use of the Internet expands, many companies and Internet users are concerned that some governments will impose extensive regulations on the Internet and electronic commerce. Potential areas of problematic regulation include taxes and duties, restrictions on the type of information transmitted, control over standards development, licensing requirements and rate regulation of service providers. Indeed, signs of these types of commerce-inhibiting actions already are appearing in many nations. Preempting these harmful actions before they take root is a strong motivation for the strategy outlined in this paper.

Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and -- at least as important -- when not to act, will be crucial to the development of electronic commerce. This report articulates the Administration's vision for the emergence of the GII as a vibrant global marketplace by suggesting a set of principles, presenting a series of policies, and establishing a road map for international discussions and agreements to facilitate the growth of commerce on the Internet.

PRINCIPLES

1. The private sector should lead.

Though government played a role in financing the initial development of the Internet, its expansion has been driven primarily by the private sector. For electronic commerce to flourish, the private sector must continue to lead. Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry.

Accordingly, governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them. Where government action or intergovernmental agreements are necessary, on taxation for example, private sector participation should be a formal part of the policy making process.

2. Governments should avoid undue restrictions on electronic commerce.

Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Unnecessary regulation of commercial activities will distort development of the electronic marketplace by decreasing the supply and raising the cost of products and services for consumers the world over. Business models must evolve rapidly to keep pace with the break-neck speed of change in the technology; government attempts to regulate are likely to be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific.

Accordingly, governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet.

3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.

In some areas, government agreements may prove necessary to facilitate electronic commerce and protect consumers. In these cases, governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation. This may involve states as well as national governments. Where government intervention is necessary to facilitate electronic commerce, its goal should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution.

4. Governments should recognize the unique qualities of the Internet.

The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. These same characteristics pose significant logistical and technological challenges to existing regulatory models, and governments should tailor their policies accordingly.

Electronic commerce faces significant challenges where it intersects with existing regulatory schemes. We should not assume, for example, that the regulatory frameworks established over

the past sixty years for telecommunications, radio and television fit the Internet. Regulation should be imposed only as a necessary means to achieve an important goal on which there is a broad consensus. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.

5. Electronic Commerce over the Internet should be facilitated on a global basis.

The Internet is emerging as a global marketplace. The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides.

ISSUES

This paper covers nine areas where international agreements are needed to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace. Although there are significant areas of overlap, these items can be divided into three main subgroups: financial issues, legal issues, and market access issues.

Financial Issues

- customs and taxation
- electronic payments

Legal Issues

- 'Uniform Commercial Code' for electronic commerce
- intellectual property protection
- privacy
- security

Market Access Issues

- telecommunications infrastructure and information technology
- content
- technical standards

I. Financial Issues

1. CUSTOMS AND TAXATION

For over 50 years, nations have negotiated tariff reductions because they have recognized that the economies and citizens of all nations benefit from freer trade. Given this recognition, and

because the Internet is truly a global medium, it makes little sense to introduce tariffs on goods and services delivered over the Internet.

Further, the Internet lacks the clear and fixed geographic lines of transit that historically have characterized the physical trade of goods. Thus, while it remains possible to administer tariffs for products ordered over the Internet but ultimately delivered via surface or air transport, the structure of the Internet makes it difficult to do so when the product or service is delivered electronically.

Nevertheless, many nations are looking for new sources of revenue, and may seek to levy tariffs on global electronic commerce.

Therefore, the United States will advocate in the World Trade Organization (WTO) and other appropriate international fora that the Internet be declared a tariff-free environment whenever it is used to deliver products or services. This principle should be established quickly before nations impose tariffs and before vested interests form to protect those tariffs.

In addition, the United States believes that no new taxes should be imposed on Internet commerce. The taxation of commerce conducted over the Internet should be consistent with the established principles of international taxation, should avoid inconsistent national tax jurisdictions and double taxation, and should be simple to administer and easy to understand. Any taxation of Internet sales should follow these principles:

- It should neither distort nor hinder commerce. No tax system should discriminate among types of commerce, nor should it create incentives that will change the nature or location of transactions.
- The system should be simple and transparent. It should be capable of capturing the overwhelming majority of appropriate revenues, be easy to implement, and minimize burdensome record keeping and costs for all parties.
- The system should be able to accommodate tax systems used by the United States and our international partners today.

Wherever feasible, we should look to existing taxation concepts and principles to achieve these goals.

Any such taxation system will have to accomplish these goals in the context of the Internet's special characteristics -- the potential anonymity of buyer and seller, the capacity for multiple small transactions, and the difficulty of associating online activities with physically defined locations.

To achieve global consensus on this approach, the United States, through the Treasury Department, is participating in discussions on the taxation of electronic commerce through the

Organization for Economic Cooperation and Development (OECD), the primary forum for cooperation in international taxation.

The Administration is also concerned about possible moves by state and local tax authorities to target electronic commerce and Internet access. The uncertainties associated with such taxes and the inconsistencies among them could stifle the development of Internet commerce. The Administration believes that the same broad principles applicable to international taxation, such as not hindering the growth of electronic commerce and neutrality between conventional and electronic commerce, should be applied to subfederal taxation. No new taxes should be applied to electronic commerce, and states should coordinate their allocation of income derived from electronic commerce. Of course, implementation of these principles may differ at the subfederal level where indirect taxation plays a larger role.

Before any further action is taken, states and local governments should cooperate to develop a uniform, simple approach to the taxation of electronic commerce, based on existing principles of taxation where feasible.

2. ELECTRONIC PAYMENT SYSTEMS

New technology has made it possible to pay for goods and services over the Internet. Some of the methods would link existing electronic banking and payment systems, including credit and debit card networks, with new retail interfaces via the Internet. Electronic money, based on stored-value, smart card, or other technologies, is also under development. Substantial private sector investment and competition is spurring an intense period of innovation that should benefit consumers and businesses wishing to engage in global electronic commerce.

At this early stage in the development of electronic payment systems, the commercial and technological environment is changing rapidly. It would be hard to develop policy that is both timely and appropriate. For these reasons, inflexible and highly prescriptive regulations and rules are inappropriate and potentially harmful. Rather, in the near term, case-by-case monitoring of electronic payment experiments is preferred.

From a longer term perspective, however, the marketplace and industry self-regulation alone may not fully address all issues. For example, government action may be necessary to ensure the safety and soundness of electronic payment systems, to protect consumers, or to respond to important law enforcement objectives.

The United States, through the Department of the Treasury, is working with other governments in international fora to study the global implications of emerging electronic payment systems. A number of organizations are already working on important aspects of electronic banking and payments. Their analyses will contribute to a better understanding of how electronic payment systems will affect global commerce and banking.

The Economic Communique issued at the Lyon Summit by the G-7 Heads of State called for a cooperative study of the implications of new, sophisticated retail electronic payment systems. In response, the G-10 deputies formed a Working Party, with representation from finance ministries and central banks (in consultation with law enforcement authorities). The Working Party is chaired by a representative from the U.S. Treasury Department, and tasked to produce a report that identifies common policy objectives among the G-10 countries and analyzes the national approaches to electronic commerce taken to date.

As electronic payment systems develop, governments should work closely with the private sector to inform policy development, and ensure that governmental activities flexibly accommodate the needs of the emerging marketplace.

II. Legal Issues

3. 'UNIFORM COMMERCIAL CODE' FOR ELECTRONIC COMMERCE

In general, parties should be able to do business with each other on the Internet under whatever terms and conditions they agree upon.

Private enterprise and free markets have typically flourished, however, where there are predictable and widely accepted legal environments supporting commercial transactions. To encourage electronic commerce, the U.S. government should support the development of both a domestic and global uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide. Fully informed buyers and sellers could voluntarily agree to form a contract subject to this uniform legal framework, just as parties currently choose the body of law that will be used to interpret their contract.

Participants in the marketplace should define and articulate most of the rules that will govern electronic commerce. To enable private entities to perform this task and to fulfill their roles adequately, governments should encourage the development of simple and predictable domestic and international rules and norms that will serve as the legal foundation for commercial activities in cyberspace.

In the United States, every state government has adopted the Uniform Commercial Code (UCC), a codification of substantial portions of commercial law. The National Conference of Commissioners of Uniform State Law (NCCUSL) and the American Law Institute, domestic sponsors of the UCC, already are working to adapt the UCC to cyberspace. Private sector organizations, including the American Bar Association (ABA) along with other interest groups, are participants in this process. Work is also ongoing on a proposed electronic contracting and records act for transactions not covered by the UCC. The Administration supports the prompt consideration of these proposals, and the adoption of uniform legislation by all states. Of

course, any such legislation will be designed to accommodate ongoing and possible future global initiatives.

Internationally, the United Nations Commission on International Trade Law (UNCITRAL) has completed work on a model law that supports the commercial use of international contracts in electronic commerce. This model law establishes rules and norms that validate and recognize contracts formed through electronic means, sets default rules for contract formation and governance of electronic contract performance, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings.

The United States Government supports the adoption of principles along these lines by all nations as a start to defining an international set of uniform commercial principles for electronic commerce. We urge UNCITRAL, other appropriate international bodies, bar associations, and other private sector groups to continue their work in this area.

The following principles should, to the extent possible, guide the drafting of rules governing global electronic commerce:

- parties should be free to order the contractual relationship between themselves as they see fit;
- rules should be technology-neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future);
- existing rules should be modified and new rules should be adopted only as necessary or substantially desirable to support the use of electronic technologies; and
- the process should involve the high-tech commercial sector as well as businesses that have not yet moved online.

With these principles in mind, UNCITRAL, UNIDROIT, and the International Chamber of Commerce (ICC), and others should develop additional model provisions and uniform fundamental principles designed to eliminate administrative and regulatory barriers and to facilitate electronic commerce by:

- encouraging governmental recognition, acceptance and facilitation of electronic communications (i.e., contracts, notarized documents, etc.);
- encouraging consistent international rules to support the acceptance of electronic signatures and other authentication procedures; and
- promoting the development of adequate, efficient, and effective alternate dispute resolution mechanisms for global commercial transactions.

The expansion of global electronic commerce also depends upon the participants, ability to achieve a reasonable degree of certainty regarding their exposure to liability for any damage or injury that might result from their actions. Inconsistent local tort laws, coupled with uncertainties regarding jurisdiction, could substantially increase litigation and create unnecessary costs that ultimately will be born by consumers. The U.S. should work closely with other nations to clarify applicable jurisdictional rules and to generally favor and enforce contract provisions that allow parties to select substantive rules governing liability.

Finally, the development of global electronic commerce provides an opportunity to create legal rules that allow business and consumers to take advantage of new technology to streamline and automate functions now accomplished manually. For example, consideration should be given to establishing electronic registries.

The Departments of Commerce and State will continue to organize U.S. participation in these areas with a goal of achieving substantive international agreement on model law within the next two years. NCCUSL and the American Law Institute, working with the American Bar Association and other interested groups, are urged to continue their work to develop complementary domestic and international efforts.

4. INTELLECTUAL PROPERTY PROTECTION

Commerce on the Internet often will involve the sale and licensing of intellectual property. To promote this commerce, sellers must know that their intellectual property will not be stolen and buyers must know that they are obtaining authentic products.

International agreements that establish clear and effective copyright, patent, and trademark protection are therefore necessary to prevent piracy and fraud. While technology, such as encryption, can help combat piracy, an adequate and effective legal framework also is necessary to deter fraud and the theft of intellectual property, and to provide effective legal recourse when these crimes occur. Increased public education about intellectual property in the information age will also contribute to the successful implementation and growth of the GII.

Copyrights

There are several treaties that establish international norms for the protection of copyrights, most notably the Berne Convention for the Protection of Literary and Artistic Works. These treaties link nearly all major trading nations and provide them with a means of protecting, under their own laws, each other's copyrighted works and sound recordings.

In December 1996, the World Intellectual Property Organization (WIPO) updated the Berne Convention and provided new protection for performers and producers of sound recordings by adopting two new treaties. The two treaties -- the WIPO Copyright Treaty and the WIPO

Performances and Phonograms Treaty -- will greatly facilitate the commercial applications of online digital communications over the GII.

Both treaties include provisions relating to technological protection, copyright management information, and the right of communication to the public, all of which are indispensable for an efficient exercise of rights in the digital environment. The U.S. Government recognizes private sector efforts to develop international and domestic standards in these areas. The Administration understands the sensitivities associated with copyright management information and technological protection measures, and is working to tailor implementing legislation accordingly.

Both treaties also contain provisions that permit nations to provide for exceptions to rights in certain cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author (e.g., "fair use"). These provisions permit members to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. These provisions permit members to devise new exceptions and limitations that are appropriate in the digital network environment, but neither reduce nor extend the scope of applicability of the limitations and exceptions permitted by the Berne Convention.

The Administration is drafting legislation to implement the new WIPO treaties, and looks forward to working with the Senate on their ratification.

The two new WIPO treaties do not address issues of online service provider liability, leaving them to be determined by domestic legislation. The Administration looks forward to working with Congress as these issues are addressed and supports efforts to achieve an equitable and balanced solution that is agreeable to interested parties and consistent with international copyright obligations.

The adoption of the two new WIPO treaties represents the attainment of one of the Administration's significant intellectual property objectives. The U.S. Government will continue to work for appropriate copyright protection for works disseminated electronically. The Administration's copyright-related objectives will include:

- encouraging countries to fully and immediately implement the obligations contained in the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS);
- seeking immediate U.S. ratification and deposit of the instruments of accession to the two new WIPO treaties and implementation of the obligations in these treaties in a balanced and appropriate way as soon as possible;
- encouraging other countries to join the two new WIPO treaties and to implement fully the treaty obligations as soon as possible; and

- ensuring that U.S. trading partners establish laws and regulations that provide adequate and effective protection for copyrighted works, including motion pictures, computer software, and sound recordings, disseminated via the GII, and that these laws and regulations are fully implemented and actively enforced.

The United States will pursue these international objectives through bilateral discussions and multilateral discussions at WIPO and other appropriate fora and will encourage private sector participation in these discussions.

Sui Generis Protection of Databases

The December 1996 WIPO Conference in Geneva did not take up a proposed treaty to protect the non-original elements of databases. Instead, the Conference called for a meeting, subsequently held, to discuss preliminary steps to study proposals to establish sui generis database protection.

Based on the brief discussion of sui generis database protection that took place before and during the Diplomatic Conference, it is clear that more discussion of the need for and the nature of such protection is necessary domestically and internationally.

The Administration will seek additional input from, among others, the scientific, library, and academic communities and the commercial sector, in order to develop U.S. policy with respect to sui generis database protection.

Patents

Development of the GII will both depend upon and stimulate innovation in many fields of technology, including computer software, computer hardware, and telecommunications. An effectively functioning patent system that encourages and protects patentable innovations in these fields is important for the overall success of commerce over the Internet. Consistent with this objective, the U.S. Patent and Trademark Office (PTO) will (1) significantly enhance its collaboration with the private sector to assemble a larger, more complete collection of prior art (both patent and non-patent publications), and provide its patent examiners better access to prior art in GII-related technologies; (2) train its patent examiners in GII-related technologies to raise and maintain their level of technical expertise; and (3) support legislative proposals for early publication of pending patent applications, particularly in areas involving fast moving technology.

To create a reliable environment for electronic commerce, patent agreements should:

- prohibit member countries from authorizing parties to exploit patented inventions related to the GII without the patent owner's authority (i.e., disapproval of compulsory licensing of GII-related technology except to remedy a practice determined after judicial or administrative process to be anti-competitive);
- require member countries to provide adequate and effective protection for patentable subject matter important to the development and success of the GII; and
- establish international standards for determining the validity of a patent claim.

The United States will pursue these objectives internationally. Officials of the European, Japanese, and United States Patent Offices meet, for example, each year to foster cooperation on patent-related issues. The United States will recommend at the next meeting that a special committee be established within the next year to make recommendations on GII-related patent issues.

In a separate venue, one hundred countries and international intergovernmental organizations participate as members of WIPO's permanent committee on industrial property information (PCIPI). The United States will attempt to establish a working group of this organization to address GII-related patent issues.

Trademark and Domain Names

Trademark rights are national in scope and conflicts may arise where the same or similar trademarks for similar goods or services are owned by different parties in different countries. Countries may also apply different standards for determining infringement.

Conflicts have arisen on the GII where third parties have registered Internet domain names that are the same as, or similar to, registered or common law trademarks. An Internet domain name functions as a source identifier on the Internet. Ordinarily, source identifiers, like addresses, are not protected intellectual property (i.e., a trademark) per se. The use of domain names as source identifiers has burgeoned, however, and courts have begun to attribute intellectual property rights to them, while recognizing that misuse of a domain name could significantly infringe, dilute, and weaken valuable trademark rights.

To date, conflicts between trademark rights and domain names have been resolved through negotiations and/or litigation. It may be possible to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis without the need to litigate. This could create a more stable business environment on the Internet. Accordingly, the United States will support efforts already underway to create domestic and international fora for discussion of Internet-related trademark issues. The Administration also plans to seek public input on the resolution of trademark disputes in the context of domain names.

Governance of the domain name system (DNS) raises other important issues unrelated to intellectual property. The Administration supports private efforts to address Internet governance issues including those related to domain names and has formed an interagency working group under the leadership of the Department of Commerce to study DNS issues. The working group will review various DNS proposals, consulting with interested private sector, consumer, professional, congressional and state government and international groups. The group will consider, in light of public input, (1) what contribution government might make, if any, to the development of a global competitive, market-based system to register Internet domain names, and (2) how best to foster bottom-up governance of the Internet.

5. PRIVACY

Americans treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the GII,s great promise -- that it facilitates the collection, re-use, and instantaneous transmission of information -- can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.

At the same time, fundamental and cherished principles like the First Amendment, which is an important hallmark of American democracy, protect the free flow of information. Commerce on the GII will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information.

In June of 1995, the Privacy Working Group of the United States government Information Infrastructure Task Force (IITF) issued a report entitled, *PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: Principles for Providing and Using Personal Information*. The report recommends a set of principles (the "Privacy Principles") to govern the collection, processing, storage, and re-use of personal data in the information age.

These Privacy Principles, which build on the Organization for Economic Cooperation and Development's GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER DATA FLOW OF PERSONAL DATA and incorporate principles of fair information practices, rest on the fundamental precepts of awareness and choice:

- Data-gatherers should inform consumers what information they are collecting, and how they intend to use such data; and
- Data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information.

Disclosure by data-gatherers is designed to stimulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for, what steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have. Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate.

In addition, the Privacy Principles identify three values to govern the way in which personal information is acquired, disclosed and used online -- information privacy, information integrity, and information quality. First, an individual's reasonable expectation of privacy regarding access to and use of, his or her personal information should be assured. Second, personal information should not be improperly altered or destroyed. And, third, personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used.

Under these principles, consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information.

In April, 1997, the Information Policy Committee of the IITF issued a draft paper entitled Options For Promoting Privacy on the National Information Infrastructure. The paper surveys information practices in the United States and solicits public comment on the best way to implement the Privacy Principles. The IITF goal is to find a way to balance the competing values of personal privacy and the free flow of information in a digital democratic society.

Meanwhile, other federal agencies have studied privacy issues in the context of specific industry sectors. In October 1995, for example, the National Telecommunications and Information Administration (NTIA) issued a report entitled Privacy and the NII: Safeguarding Telecommunications-Related Personal Information. It explores the application of the Privacy Principles in the context of telecommunications and online services and advocates a voluntary framework based on notice and consent. On January 6, 1997, the FTC issued a staff report entitled Public Workshop on Consumer Privacy on the Global Information Infrastructure. The report, which focuses on the direct marketing and advertising industries, concludes that notice, choice, security, and access are recognized as necessary elements of fair information practices online. In June of 1997, the FTC held four days of hearings on technology tools and industry self-regulation regimes designed to enhance personal privacy on the Internet.

The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution.

The Administration also anticipates that technology will offer solutions to many privacy concerns in the online environment, including the appropriate use of anonymity. If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online.

The Administration is particularly concerned about the use of information gathered from children, who may lack the cognitive ability to recognize and appreciate privacy concerns. Parents should be able to choose whether or not personally identifiable information is collected from or about their children. We urge industry, consumer, and child-advocacy groups working together to use a mix of technology, self-regulation, and education to provide solutions to the particular dangers arising in this area and to facilitate parental choice. This problem warrants prompt attention. Otherwise, government action may be required.

Privacy concerns are being raised in many countries around the world, and some countries have enacted laws, implemented industry self-regulation, or instituted administrative solutions designed to safeguard their citizens' privacy. Disparate policies could emerge that might disrupt transborder data flows. For example, the European Union (EU) has adopted a Directive that prohibits the transfer of personal data to countries that, in its view, do not extend adequate privacy protection to EU citizens.

To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled.

The United States will continue policy discussions with the EU nations and the European Commission to increase understanding about the U.S. approach to privacy and to assure that the criteria they use for evaluating adequacy are sufficiently flexible to accommodate our approach. These discussions are led by the Department of Commerce, through NTIA, and the State Department, and include the Executive Office of the President, the Treasury Department, the Federal Trade Commission (FTC) and other relevant federal agencies. NTIA is also working with the private sector to assess the impact that the implementation of the EU Directive could have on the United States.

The United States also will enter into a dialogue with trading partners on these issues through existing bilateral fora as well as through regional fora such as the Asia Pacific Economic Cooperation (APEC) forum, the Summit of the Americas, the North American Free Trade Agreement (NAFTA), and the Inter-American Telecommunications Commission (CITEL) of the Organization of American States, and broader multilateral organizations.

The Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.

6. SECURITY

The GII must be secure and reliable. If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce. A secure GII requires:

- (1) secure and reliable telecommunications networks;
- (2) effective means for protecting the information systems attached to those networks; (3) effective means for authenticating and ensuring confidentiality of electronic information to protect data from unauthorized use; and
- (4) well trained GII users who understand how to protect their systems and their data.

There is no single "magic" technology or technique that can ensure that the GII will be secure and reliable. Accomplishing that goal requires a range of technologies (encryption, authentication, password controls, firewalls, etc.) and effective, consistent use of those technologies, all supported globally by trustworthy key and security management infrastructures.
Of particular importance is the development of trusted certification services that support the digital signatures that will permit users to know whom they are communicating with on the Internet. Both signatures and confidentiality rely on the use of cryptographic keys. To promote the growth of a trusted electronic commerce environment, the Administration is encouraging the development of a voluntary, market-driven key management infrastructure that will support authentication, integrity, and confidentiality.

Encryption products protect the confidentiality of stored data and electronic communications by making them unreadable without a decryption key. But strong encryption is a double-edged sword. Law abiding citizens can use strong encryption to protect their trade secrets and personal records. But those trade secrets and personal records could be lost forever if the decrypt key is lost. Depending upon the value of the information, the loss could be quite substantial. Encryption can also be used by criminals and terrorists to reduce law enforcement capabilities to read their communications. Key recovery based encryption can help address some of these issues.

In promoting robust security needed for electronic commerce, the Administration has already taken steps that will enable trust in encryption and provide the safeguards that users and society will need. The Administration, in partnership with industry, is taking steps to promote the development of market-driven standards, public-key management infrastructure services

and key recoverable encryption products. Additionally, the Administration has liberalized export controls for commercial encryption products while protecting public safety and national security interests.

The Administration is also working with Congress to ensure legislation is enacted that would facilitate development of voluntary key management infrastructures and would govern the release of recovery information to law enforcement officials pursuant to lawful authority. The U.S. government will work internationally to promote development of market-driven key management infrastructure with key recovery. Specifically, the U.S. has worked closely within the OECD to develop international guidelines for encryption policies and will continue to promote the development of policies to provide a predictable and secure environment for global electronic commerce.

III. Market Access Issues

7. TELECOMMUNICATIONS INFRASTRUCTURE AND INFORMATION TECHNOLOGY

Global electronic commerce depends upon a modern, seamless, global telecommunications network and upon the computers and information appliances that connect to it. Unfortunately, in too many countries, telecommunications policies are hindering the development of advanced digital networks. Customers find that telecommunications services often are too expensive, bandwidth is too limited, and services are unavailable or unreliable. Likewise, many countries maintain trade barriers to imported information technology, making it hard for both merchants and customers to purchase the computers and information systems they need to participate in electronic commerce.

In order to spur the removal of barriers, in March 1994, Vice President Gore spoke to the World Telecommunications Development Conference in Buenos Aires. He articulated several principles that the U.S. believes should be the foundation for government policy, including:

- (1) encouraging private sector investment by privatizing government-controlled telecommunications companies;
- (2) promoting and preserving competition by introducing competition to monopoly phone markets, ensuring interconnection at fair prices, opening markets to foreign investment, and enforcing anti-trust safeguards;
- (3) guaranteeing open access to networks on a non-discriminatory basis, so that GII users have access to the broadest range of information and services; and
- (4) implementing, by an independent regulator, pro-competitive and flexible regulation that keeps pace with technological development.

Domestically, the Administration recognizes that there are various constraints in the present network that may impede the evolution of services requiring higher bandwidth. Administration

initiatives include Internet II, or Next Generation Internet. In addition, the FCC has undertaken several initiatives designed to stimulate bandwidth expansion, especially to residential and small/home office customers.

The goal of the United States will be to ensure that online service providers can reach end-users on reasonable and nondiscriminatory terms and conditions. Genuine market opening will lead to increased competition, improved telecommunications infrastructures, more customer choice, lower prices and increased and improved services.

Areas of concern include:

- **Leased lines:** Data networks of most online service providers are constructed with leased lines that must be obtained from national telephone companies, often monopolies or governmental entities. In the absence of effective competition, telephone companies may impose artificially inflated leased line prices and usage restrictions that impede the provision of service by online service providers.
- **Local loops pricing:** To reach their subscribers, online service providers often have no choice but to purchase local exchange services from monopoly or government-owned telephone companies. These services also are often priced at excessive rates, inflating the cost of data services to customers.
- **Interconnection and unbundling:** Online service providers must be able to interconnect with the networks of incumbent telecommunication companies so that information can pass seamlessly between all users of the network. Monopolies or dominant telephone companies often price interconnection well above cost, and refuse to interconnect because of alleged concerns about network compatibility or absence of need for other providers.
- **Attaching equipment to the network:** Over the years, some telecommunication providers have used their monopoly power to restrict the connection of communication or technology devices to the network. Even when the monopoly has been broken, a host of unnecessary burdensome "type acceptance" practices have been used to retard competition and make it difficult for consumers to connect.
- **Internet voice and multimedia:** Officials of some nations claim that "real time" services provided over the Internet are "like services" to traditionally regulated voice telephony and broadcasting, and therefore should be subject to the same regulatory restrictions that apply to those traditional services. In some countries, these providers must be licensed, as a way to control both the carriage and content offered. Such an approach could hinder the development of new technologies and new services.

In addition, countries have different levels of telecommunications infrastructure development, which may hinder the global provision and use of some Internet-based services. The Administration believes that the introduction of policies promoting foreign investment,

competition, regulatory flexibility and open access will support infrastructure development and the creation of more data-friendly networks.

To address these issues, the Administration successfully concluded the WTO Basic Telecommunications negotiations, which will ensure global competition in the provision of basic telecommunication services and will address the many underlying issues affecting online service providers. During those negotiations, the U.S. succeeded in ensuring that new regulatory burdens would not be imposed upon online service providers that would stifle the deployment of new technologies and services.

As the WTO Agreement is implemented, the Administration will seek to ensure that new rules of competition in the global communications marketplace will be technology neutral and will not hinder the development of electronic commerce. In particular, rules for licensing new technologies and new services must be sufficiently flexible to accommodate the changing needs of consumers while allowing governments to protect important public interest objectives like universal service. In this context, rules to promote such public interest objectives should not fall disproportionately on any one segment of the telecommunications industry or on new entrants. The Administration will also seek effective implementation of the Information Technology Agreement concluded by the members of the WTO in March 1997, which is designed to remove tariffs on almost all types of information technology. Building on this success, and with the encouragement of U.S. companies, the administration is developing plans for ITA II, in which it will to seek to remove remaining tariffs on, and existing non-tariff barriers to, information technology goods and services. In addition, the Administration is committed to finding other ways to streamline requirements to demonstrate product conformity, including through Mutual Recognition Agreements (MRAS) that can eliminate the need for a single product to be certified by different standards laboratories across national borders.

Bilateral exchanges with individual foreign governments, regional fora such as APEC and CITEL, and multilateral fora such as the OECD and ITU, and various other fora (i.e. international alliances of private businesses, the International Organization of Standardization [ISO], the International Electrotechnical Commission [IEC]), also will be used for international discussions on telecommunication-related Internet issues and removing trade barriers that inhibit the export of information technology. These issues include the terms and conditions governing the exchange of online traffic, addressing, and reliability. In all fora, U.S. Government positions that might influence Internet pricing, service delivery options or technical standards will reflect the principles established in this paper and U.S. Government representatives will survey the work of their study groups to ensure that this is the case.

In addition, many Internet governance issues will best be dealt with by means of private, open standards processes and contracts involving participants from both government and the private sector. The U.S. government will support industry initiatives aimed at achieving the important goals outlined in this paper.

8. CONTENT

The U.S. government supports the broadest possible free flow of information across international borders. This includes most informational material now accessible and transmitted through the Internet, including through World Wide Web pages, news and other information services, virtual shopping malls, and entertainment features, such as audio and video products, and the arts. This principle extends to information created by commercial enterprises as well as by schools, libraries, governments and other nonprofit entities.

In contrast to traditional broadcast media, the Internet promises users greater opportunity to shield themselves and their children from content they deem offensive or inappropriate. New technology, for example, may enable parents to block their children's access to sensitive information or confine their children to pre-approved websites.

To the extent, then, that effective filtering technology becomes available, content regulations traditionally imposed on radio and television would not need to be applied to the Internet. In fact, unnecessary regulation could cripple the growth and diversity of the Internet.

The Administration therefore supports industry self-regulation, adoption of competing ratings systems, and development of easy-to-use technical solutions (e.g., filtering technologies and age verification systems) to assist in screening information online.

There are four priority areas of concern:

- **Regulation of content.** Companies wishing to do business over the Internet, and to provide access to the Internet (including U.S. online service providers with foreign affiliates or joint ventures) are concerned about liability based on the different policies of every country through which their information may travel.
- Countries that are considering or have adopted laws to restrict access to certain types of content through the Internet emphasize different concerns as a result of cultural, social, and political difference. These different laws can impede electronic commerce in the global environment.
- The Administration is concerned about Internet regulation of this sort, and will develop an informal dialogue with key trading partners on public policy issues such as hate speech, violence, sedition, pornography and other content to ensure that differences in national regulation, especially those undertaken to foster cultural identity, do not serve as disguised trade barriers.
- **Foreign content quotas.** Some countries currently require that a specific proportion of traditional broadcast transmission time be devoted to "domestically produced" content. Problems could arise on the Internet if the definition of "broadcasting" is changed to extend these current regulations to "new services." Countries also might decide to

regulate Internet content and establish restrictions under administrative authority, rather than under broadcast regulatory structures.

- The Administration will pursue a dialogue with other nations on how to promote content diversity, including cultural and linguistic diversity, without limiting content. These discussions could consider promotion of cultural identity through subsidy programs that rely solely on general tax revenues and that are implemented in a nondiscriminatory manner.
- **Regulation of advertising.** Advertising will allow the new interactive media to offer more affordable products and services to a wider, global audience. Some countries stringently restrict the language, amount, frequency, duration, and type of tele-shopping and advertising spots used by advertisers. In principle, the United States does not favor such regulations. While recognizing legitimate cultural and social concerns, these concerns should not be invoked to justify unnecessarily burdensome regulation of the Internet.
- There are laws in many countries around the world that require support for advertising claims. Advertising industry self-regulation also exists in many countries around the globe. Truthful and accurate advertising should be the cornerstone of advertising on all media, including the Internet.
- A strong body of cognitive and behavioral research demonstrates that children are particularly vulnerable to advertising. As a result, the U.S. has well established rules (self-regulatory and otherwise) for protecting children from certain harmful advertising practices. The Administration will work with industry and childrens advocates to ensure that these protections are translated to and implemented appropriately in the online media environment.
- The rules of the "country-of-origin" should serve as the basis for controlling Internet advertising to alleviate national legislative roadblocks and trade barriers.
- **Regulation to prevent fraud.** Recently, there have been a number of cases where fraudulent information on companies and their stocks, and phony investment schemes have been broadcast on the Internet. The appropriate federal agencies (i.e., Federal Trade Commission and the Securities and Exchange Commission) are determining whether new regulations are needed to prevent fraud over the Internet.
- In order to realize the commercial and cultural potential of the Internet, consumers must have confidence that the goods and services offered are fairly represented, that they will get what they pay for, and that recourse or redress will be available if they do not. This is an area where government action is appropriate.

The Administration will explore opportunities for international cooperation to protect consumers and to prosecute false, deceptive, and fraudulent commercial practices in cyberspace.

Federal agencies such as the Department of State, U.S. Trade Representative (USTR), the Commerce Department (NTIA), the FTC, the Office of Consumer Affairs and others have already engaged in efforts to promote such positions, through both bilateral and multilateral channels,

including through the OECD, the G-7 Information Society and Development Conference, the Latin American Telecommunications Summits, and the Summit of the Americas process, as well as APEC Telecommunications Ministerials. All agencies participating in such fora will focus on pragmatic solutions based upon the principles in this paper to issues related to content control.

9. TECHNICAL STANDARDS

Standards are critical to the long term commercial success of the Internet as they can allow products and services from different vendors to work together. They also encourage competition and reduce uncertainty in the global marketplace. Premature standardization, however, can "lock in" outdated technology. Standards also can be employed as de facto non-tariff trade barriers, to "lock out" non-indigenous businesses from a particular national market. The United States believes that the marketplace, not governments, should determine technical standards and other mechanisms for interoperability. Technology is moving rapidly and government attempts to establish technical standards to govern the Internet would only risk inhibiting technological innovation. The United States considers it unwise and unnecessary for governments to mandate standards for electronic commerce. Rather, we urge industry driven multilateral fora to consider technical standards in this area.

To ensure the growth of global electronic commerce over the Internet, standards will be needed to assure reliability, interoperability, ease of use and scalability in areas such as:

- electronic payments;
- security (confidentiality, authentication, data integrity, access control, non-repudiation);
- security services infrastructure (e.g., public key certificate authorities);
- electronic copyright management systems;
- video and data-conferencing;
- high-speed network technologies (e.g., Asynchronous Transfer Mode, Synchronous Digital Hierarchy); and
- digital object and data interchange.

There need not be one standard for every product or service associated with the GII, and technical standards need not be mandated. In some cases, multiple standards will compete for marketplace acceptance. In other cases, different standards will be used in different circumstances.

The prevalence of voluntary standards on the Internet, and the medium's consensus-based process of standards development and acceptance are stimulating its rapid growth. These standards flourish because of a non-bureaucratic system of development managed by technical practitioners working through various organizations. These organizations require demonstrated deployment of systems incorporating a given standard prior to formal acceptance, but the process facilitates rapid deployment of standards and can accommodate evolving standards as

well. Only a handful of countries allow private sector standards development; most rely on government-mandated solutions, causing these nations to fall behind the technological cutting edge and creating non-tariff trade barriers.

Numerous private sector bodies have contributed to the process of developing voluntary standards that promote interoperability. The United States has encouraged the development of voluntary standards through private standards organizations, consortia, testbeds and R&D activities. The U.S. government also has adopted a set of principles to promote acceptance of domestic and international voluntary standards.

While no formal government-sponsored negotiations are called for at this time, the United States will use various fora (i.e., international alliances of private businesses, the International Organization for Standardization [ISO], the International Electrotechnical Commission [IEC], International Telecommunications Union [ITU], etc.) to discourage the use of standards to erect barriers to free trade on the developing GII. The private sector should assert global leadership to address standards setting needs. The United States will work through intergovernmental organizations as needed to monitor and support private sector leadership.

A COORDINATED STRATEGY

The success of electronic commerce will require an effective partnership between the private and public sectors, with the private sector in the lead. Government participation must be coherent and cautious, avoiding the contradictions and confusions that can sometimes arise when different governmental agencies individually assert authority too vigorously and operate without coordination.

The variety of issues being raised, the interaction among them, and the disparate fora in which they are being addressed will necessitate a coordinated, targeted governmental approach to avoid inefficiencies and duplication in developing and reviewing policy.

An interagency team will continue to meet in order to monitor progress and update this strategy as events unfold. Sufficient resources will be committed to allow rapid and effective policy implementation.

The process of further developing and implementing the strategy set forth in this paper is as important as the content of the paper itself. The U.S. Government will consult openly and often, with groups representing industry, consumers and Internet users, Congress, state and local governments, foreign governments, and international organizations as we seek to update and implement this paper in the coming years.

Private sector leadership accounts for the explosive growth of the Internet today, and the success of electronic commerce will depend on continued private sector leadership. Accordingly,

the Administration also will encourage the creation of private fora to take the lead in areas requiring self-regulation such as privacy, content ratings, and consumer protection and in areas such as standards development, commercial code, and fostering interoperability.

The strategy outlined in this paper will be updated and new releases will be issued as changes in technology and the marketplace teach us more about how to set the optimal environment in which electronic commerce and community can flourish.

There is a great opportunity for commercial activity on the Internet. If the private sector and governments act appropriately, this opportunity can be realized for the benefit of all people.

A Framework For Global Electronic Commerce
President William J. Clinton
Vice President Albert Gore, Jr.
Washington, D.C.