SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Canada-United States Law Journal

Volume 29 | Issue 1 Article 35

January 2003

Security and the Economy: The North American Computer and Communication Infrastructure - U.S. Speaker

Theodore C. Theofrastous

Recommended Citation

Theodore C. Theofrastous, *Security and the Economy: The North American Computer and Communication Infrastructure - U.S. Speaker*, 29 Can.-U.S. L.J. 225 (2003)
Available at: https://scholarlycommons.law.case.edu/cuslj/vol29/iss1/35

SECURITY AND THE ECONOMY: THE NORTH AMERICAN COMPUTER AND COMMUNICATION INFRASTRUCTURE

Theodore C. Theofrastous[†]
U.S. Speaker

Out of respect for my new friend Selma's travel schedule, I have cut ten slides out of this presentation so we can move along quickly. I apologize in advance to any of you who feel that I am using too many buzz words or acronyms. I will try to explain them as I go along, but the 20-minute version of this speech is likely to suffer from abbreviation.

I have been asked to speak about the American Information Technology (IT) Infrastructure in the context of Homeland Security. As background for this topic, I will first attempt to provide some background on the many ongoing efforts to secure this infrastructure and some of the known threats that have been addressed thus far. I will then discuss the Bush administration's proposed approach to "cyber-terror" and some of the potential concerns I have regarding that approach.

If we talk about threats in the IT context, this industry or this particular infrastructure, unlike some of the others under discussion, has some well-established threats and some well-established mechanisms for dealing with those threats. Security issues raised by hackers, cyber-criminals, virus writers, spammers, spoofers, crackers, etc., represent ongoing efforts to make computer systems safe and reliable, especially in the context of the Internet. To some degree, these issues are well worn and reasonably well addressed by industry and government and would not rise to the level of becoming threats to homeland security or national defense – at least not before September 11th.

[†] Theodore C. Theofrastous is Chief Commercialization Counsel for The Cleveland Clinic Foundation. Prior to joining the Foundation, Mr. Theofrastous was an associate with the law firm of Squire, Sanders & Dempsey, L.L.P, where his practice focus included high tech and intellectual property law, specifically in the areas of e-commerce, technology transfer, licensing, corporate finance and business counseling in the information technology and life sciences fields. Before entering the practice of law, he spent more than ten years working working as a professional in the field of information technology and data communications. He is also member of the adjunct faculty at the Case Western Reserve University School of Law, where he teaches Conflict of Laws (including Internet Conflicts) and Advanced International and Foreign Legal Research. Mr. Theofrastous received his B.A. from Marlboro College and a J.D. from Case Western Reserve University.

Part of what I think we need to review in the context of homeland security is to what degree we will rely on existing technology and initiatives. We also need to think about to what degree will we throw out those existing approaches in favor of something that is more aggressive, better funded, and more challenging from a constitutional perspective.

Traditional non-terrorist threats to the American IT infrastructure are relatively well-known. From the perspective of the individual, privacy in the context of an ever-growing reliance on the Internet as the preferred medium for communication and conducting business has been an area of significant debate and investment,[1] although certainly more so prior to the current Bush administration.[2] From a commercial perspective, the cultural adoption of e-commerce, both in the business-to-consumer and the business-to-business contexts, has required standardization of a number of critical areas ranging from anti-fraud and authentication of electronic transactions[3] to the emergence a discrete regime of "cyber-law."[4] In the context of financial market and large institutions, the ever expanding flow of transaction information (e.g., automated clearing house [ACH] transactions)[5] must be protected by increasingly reliable forms of encryption and transactional fail-safes. At the national level, the Internet has completely transformed the federal government's ability to share information with the public,[6] while simultaneously providing the infrastructure for high-end applications such as the secure, run-time distribution of intelligence and national security information, which, of course, is built around commercially-available hardware and software.[7]

[1] *See, e.g., Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, ELECTRONIC PRIVACY INFORMATION CENTER (2003).

[2] *See, e.g., New FTC Chairman will Protect Consumer Privacy, but Not with New Regulations*, CONSUMER FINANCIAL SERVICES LAW REPORT, Vol. 5, No. 2 (June 27, 2001).

[3] *See, e.g.*, Electronic Signatures in Global and National Commerce Act (E-SIGN), PUB. L. NO. 106-229, 114 STAT. 464 (2000) codified at 15 U.S.C. § 7001 *et seq.*; Model statute proposed by the National Conference of Commissions in July 1999. Model Uniform Electronic Transactions Act (UETA) (1999), *available at* www.uetaonline.com/uetaoc.html

[4] *See, e.g.*, Reference materials presented by the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, U.S DEPT. OF JUSTICE, *available at* www.usdoj.gov/criminal/cybercrime/compcrime.html.

[5] *NACHA Internet Council Reports on Managing Risks of Internet Payments,* Press Release, NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION, Feb. 4, 2003, *available at* http://internetcouncil.nacha.org/docs/Internet%20Council%20Publications%20%20Risk%20 Management.doc

[6] *See, e.g., "Thomas"* the U.S. Library of Congress' website, *available at* http://thomas.loc.gov (providing legislative information on the Internet.); *Also see,* GPO Access, *available at* www.gpoaccess.gov/fr/index.html (providing free, online access to the U.S. Federal Register from 1994 through the present).

[7] *See*, e.g., Lance Ulanoff, *An Insider's Look at Homeland Security and Technology,* PC MAGAZINE, Sept. 6, 2002, *available at* www.pcmag.com/print_article/0,3048,a

Allow me to take an important a step back to look at what we are talking about when we say "computer infrastructure." I actually used something very similar to what I am going to share with you about eight years ago to explain to a Board of Directors what it means to connect across the Internet to another computer. It is a pretty simple model. Conceptually, you used to have a computer somewhere that was connected to some kind of communications medium, which is in turn connected to the external communications "web." Who knew what was out there, but the presumption used to be not very much. The communication was eventually routed to another computer connected to the same "web." In the shortest possible strokes, that is a communications network. When we talk about the Internet, we are talking about network of networks. The key hardware or buzz words that we would be dealing with here are primarily related to the concept of "routing" traffic across and between those networks. All across the Internet, information is being generated and it is being transmitted across a series of interconnect points en route to its final destination.

This does not mean, however, that traffic simply goes from point A, through point B, to point C. The best example of this is right in my own home. I live about 25 miles from Cleveland in a rural area. I was a very enthusiastic subscriber to DSL when it was introduced to the area where I live. At one point, my connection was acting up. While I could connect to lots of places on the Internet, I could not communicate with my law firm in Cleveland. The engineers at my Internet service provider and at the law firm could not find anything wrong. Naturally, I assumed the local telecom carrier was at fault. Not true. The problem was actually in a network router physically located somewhere in Texas. Traffic from my home to Cleveland was being routed along a series of some 20 hops up through Canada, down to Texas, and back up to Cleveland. Theoretically, that was the most efficient route between those two points.

Given the massive infrastructure available, this is actually not unusual. The telecommunications infrastructure becomes sort of a lattice work of individual points of connection connected to what we would generally think of as a backbone. A backbone is some wider communication medium that is being used and shared by other users. The optimized use of the major backbone providers requires that routes be less a function of geography than of the needs of the overall system. Even when we look at a single

=30737,00.asp (quoting Steve I. Cooper, Special Assistant to the President, senior director for information integration, and CIO for the Office of Homeland Security "We're working very closely with Microsoft to improve and correct some of the security deficiencies that we've found..., with Microsoft's products. It's not a secret. Microsoft knows it. And they've actually engaged very cooperatively in working collaboratively with the Federal environment to fix these things.").

"backbone" we have to acknowledge that the backbone itself is a network, consisting of numerous large capacity circuits, large capacity switches and routers, large capacity exchange points and major network access points (NAPs).

The major point is that if any one of these pieces of wire goes out, there is probably another one ready to provide an alternate route. The thing about routers is that they are smart enough to figure out if you cannot get there the way you used to get there, maybe you can get there some other way. I think if you look at the Internet from this perspective, the concept of the web is a little easier to understand. It is an interweaving of connected networks with no inherently linear design.

The reality is there is a lot of wire out there. I apologize to Selma, I think this is one of your competitor's backbone maps. This is just one carrier. In a simple regional network map the major connections inside the United States are overlaid on top of the myriad smaller interconnections. Many of these are actually looping up into Canada. Cleveland is right in the middle. From this schematic, two points are evident: one, there is a lot of wire; and two, it is difficult to locate the U.S. border. The border is not particularly relevant in this context, at least not before we started viewing this infrastructure through the homeland security lens.

If you want to take a look at the Internet, per se, it looks more really like this "skitter" graph map of major Internet backbones, created by the Cooperative Association for Internet Data Analysis and the San Diego Supercomputer Center.[8] It is difficult to interpret this graph in a geographically meaningful way, other than in terms of the amount of bandwidth and the number of circuits that are available in any given place. Comparing this graph to earlier versions, one can observe a growing whiteness in the center, which is one way to illustrate incredible continual expansion of global bandwidth. If we take a closer look at the model, you can see that the myriad of spokes are major metropolitan areas that have massive amounts of bandwidth and massive amounts of backbone going in and out of them.

Great graphics, but what does it mean? To me, it means that infrastructural terrorism does not mean "dropping a bomb" on the Internet. A terrorist could wreak havoc. A terrorist could commandeer a ship and run it into a submarine cable, but the point is there is not just one cable.[9] It will be an incident. It will be a disaster. It will cost somebody a lot of money,

[8] *See*, The AS Internet graph: A Macroscopic Visualisation of the Internet, COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS, April 1-16, 2002, *available at* www.caida.org/analysis/topology/as_core_network/AS_Network.xml

[9] *See*, *e.g.*, Global Communications Submarine Cable Map (2003), *available at* www.telegeography.com/maps/cable/japan_detail.html

but it is not the kind of thing that is likely to achieve the sort of havoc and panic that a terrorist organization is trying to achieve on a systematic basis. In a moment I will give you what I think is a good example of the type of scenario that I think might be more worthy of our attention.

Going back to my initial point, before 9-11 and homeland security, we had legitimate threats, but none that instilled "terror." Viruses were certainly a serious threat. Anyone in the audience who ever received, for instance, the "I love you" virus, which hit something like 10 million computers and cost billions depending on your perspective,[10] knows that a virus can have a serious and embarrassing impact on your use of electronic mail. The regrettable thing about most viruses is that they exploit relatively major oversights in your computer software. I actually looked at the "I love you" script, which was not particularly sophisticated. The power of the script was that it used "features" built into Microsoft Outlook to do really annoying things such as sending a copy of itself via email to everyone in your address book, deleting certain file types on your computer and refreshing itself directly from a web-based location. That virus, like other email "worms," really amounted to a sort of "death by spam," ultimately overloading the network through the exponential propagation of itself. The real downside is the resulting failure of the communications infrastructure inability to handle such high volume.

Now we have a very high level of awareness of malicious attacks; the inherent nature of the infrastructure to fail by virtue of our continual tendency to overload it; the continual expansion of the adoption of very large applications on the Internet; the dance between commerce and the individual on a privacy level and at a government level; and then the ongoing law enforcement equation of prosecuting crimes that may have evolved into the Internet context and present new challenges. For each one of these problems, there has been a very significant and very effective response – both in terms of protecting the infrastructure, as well as the systems that are dependent on and a part of that infrastructure.

If we look solely at the systems infrastructure that has evolved and the stress we have placed on it, the fact that we have adopted larger capacity and greater quantities of more wire is natural, albeit only a partial solution. From an engineering perspective, the key concept during the dot com expansion was "decentralization." Decentralization both in terms of meeting ever

[10] *See "Love Bug" Takes on the World*, CNN, May 5, 2000, *available at* www.cnn.com/2000/WORLD/europe/05/05/virus.world/; "I Love You" virus infected 45 million computers. *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987, and H.R. 4908 Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong., 16-27 (2000) (statement of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division, Dept. of Justice).

expanding demand as well as to exposure to any single point of threat. Internet-dependent companies made huge investments getting their eggs into as many baskets as possible. The intent was to move information closer to where it was needed to avoid bottlenecks and single points of failure. During this time, concepts such as collocation, multi-homing, and datacenters emerged as standard vocabulary. Entire businesses were built around cutting edge caching and mirroring technologies. At the same time, new, ambitious distributed and grid computing models emerged to leverage the capabilities of faster computers, more powerful middleware, lower latency models in communications hardware and emerging industry standards for high-end systems redundancy and disaster recovery.

During this time, the conceptual model of the Internet obviously changed quite a bit. Instead of the macro view of a computer connected to the "web" talking to another similarly connected computer, now we have to add content-specialized caching and mirrored content servers, satellite networks, database servers, etc. Say a user is performing a streaming download of World Cup video. The user may initially connect to the media from a site in the U.K., but the content is being moved around to various places in the world, across multiple channels, all in ways that are hopefully transparent to the user.

In order to protect systems, we have developed and implemented firewalls, anti-virus software, and encryption in both consumer and business environments. Sophistication of users and technicians has increased at all levels and high-end protective mechanisms have become par for the course.[11]

Of course, any time someone discovers a new gap in the operating system that you use or the hardware that you use, new solutions will have to be developed. I think it is now safe to say that this part of doing business today. The question becomes one of the cost, both direct and indirect, of these solutions relative to the threat. The Federal Bureau of Investigation (FBI) has been conducting a survey of some 800 fairly large companies over the last five years.[12]

Each year the survey attempts to capture relative perceptions regarding exposure to cyber crime, what level of damage the respondent is personally incurring, and what gathering subjective estimates of the source of attack. Whether or not you know what "IP spoofing" is, I would guess that few in this audience would review the report and say, "Oh, my God, I never thought

[11] An extremely sophisticated pc-based firewall package. *See, e.g.*, ZoneAlarm Pro, *available at* www.zonelabs.com

[12] 2003 Computer Crime and Security Survey is a joint survey conducted by the Computer Security Institute and the Federal Bureau of Investigation. Robert Richardson, *Cyber Attacks Continue, But Losses Are Down*, COMPUTER SECURITY INSTITUTE, May 29, 2003, *available at* www.gocsi.com/awareness/fbi.jhtml

of that" or "You know it never occurred to me that that is something you needed to be careful of."

Last year the survey estimated damages of approximately $200 million. That is combined across all respondents. Looking at this level of exposure over a period of five years, major incidents tend to average approximately $50 million. To be clear, $50 million is a lot of money and that kind of exposure is a serious concern. I believe it is equally clear that this is not the type of thing that provokes investment in the range of billions of dollars or further stresses some of the Constitutional limitations that the current cyber crime enforcement equation involves.

Now I am going to show you a short video clip, which I think comes much closer to depicting the kind of cyber terrorist attack with which we should probably be concerned with. The premise here is that cyber terrorism, just like any other type of terrorism, is going to be most effective if it has a systematic rather than a discreet effect. This would likely involve a large scale attack that changes your perception of safety and reliability along the lines of the potential threat posed by "Y2K," a form of terror we essentially inflicted on ourselves. What happens when you, as a consumer, are no longer entirely sure if ATMs are going to have money, that money is safe in the bank, that it is safe to trade stocks online, or do all the other things that one might normally do online. Further, what if the systems that make up our infrastructure are not making best use of the protection measures and best practices available? What if we are vulnerable just because we are being sloppy or not thinking creatively?

This video is a presentation broadcast on CSPAN where the Gartner Group and the Naval War College review the results of a joint war game simulating a coordinated attack on critical Internet infrastructure underlying the telecom and electrical grids and the financial services sector. The group within Gartner call themselves Sector 5 and war game was entitled Digital Pearl Harbor. In this clip, Annemarie Earley, a Gartner consultant, will provide an overview of the financial services attack.

(*Mr. Theofrastous played a video clip.*)

Summary of Video Clip: According to Ms. Earley, the intent of the financial services group was to confuse consumers and undermine data integrity so that the cash position of consumers and corporations was questionable. The group would begin by setting up a corporate account at a small financial institution approximately two years in advance of the attack. The group would generate a significant volume of ACH transactions over this period, letting the Federal Reserve settle those transactions, rather than getting involved directly. The target date for the attack was set for the day after Thanksgiving, 2003, with

> the following day being the busiest retail shopping day of the year and payroll for many organizations paid over the weekend (including social security, railroad retirement, etc.) This date was also attractive in that, being the Friday after Thanksgiving, the group believed that "A-List" employees would likely be on vacation, making it more likely that a flood of bogus ACH transactions would not be immediately detected and they could achieve a significant enough volume to overwhelm the federal reserve. The group decided that, particularly in the context of a multi-system attack, within two weeks, they could lower corporate and consumer confidence by making questionable Federal Reserve requirements, account balances, stock quotes, etc. The group believed that this flood could lead to a devaluation of the dollar and general sense of insecurity for a relatively small investment. One feature of the plan relied on the availability of top operatives, as the "ACH format is known by everybody, worldwide."

My point with this clip is that, depending on the level of diabolical assumption one is willing to entertain, there are certainly some things we should be considering that are not related to routers and wires. The problem that I see is two-fold. First, the real terror threats will require very creative thinking about vulnerabilities and the downstream effects massive systems attacks can have on our economy and safety. Without being glib, I am inclined to say this is only a matter of applying our best and brightest to the task. The second issue is more troublesome to me. That is, under the current administration, we face the potential of a pre- 9-11 willingness to relax the regulation of information privacy I mentioned before, potentially coupled with a post- 9-11 abridgement of certain civil rights in the interest of combating terrorism.

One initial step in weighing some of these concerns took place under the Clinton Administration, with the formation of the Critical Infrastructure Assurance Office (CIAO).[13] CIAO is now organized under the Department of Homeland Security (DHS), but the CIAO's initial approach to civil liberties is noteworthy. According to the General Statement of Principles,

[13] The Critical Infrastructure Assurance Office (CIAO) was created in response to PDD-63 (May 1998) to coordinate the government's initiatives on critical infrastructure assurance. CIAO's role was expanded by EXEC. ORDER 13231 (Oct. 16, 2001) establishing The President's Critical Infrastructure Protection Board. The mission of CIAO was to: (1) Coordinate and implement the national strategy; (2)Assess the U.S. Government's own risk exposure and dependencies on critical infrastructure; (3) Raise awareness and educate public understanding and participation in critical infrastructure protection efforts; and (4) Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors. *Id.*

whatever the CIAO does should be balanced against the rights of the citizens, e.g., the protection of proprietary data and privacy.[14] Of course, there have since been a number of acts that overstepped the kind of idealism this represents. Most visible was the FBI's Carnivore system, which was essentially designed around the concept that the FBI should be trusted to collect *ALL* possible information online.[15] Carnivore would cull out just the necessary pieces, e.g., criminally relevant information, and the remainder would be discarded. Obviously, that is a fairly controversial approach.[16]

With the introduction of homeland security, national objectives have been set to try to confront cyber terrorism.[17] In the words of the Bush administration, "Cyberspace is [the] nervous system" of the nation's critical infrastructures.[18] The objectives of the plan are four-fold: (1) Prevent cyber attacks against America's critical infrastructures; (2) Reduce national vulnerability to cyber attacks; (3) Minimize damage and recovery time from cyber attacks that do occur; and (4) Detect terrorist activities.[19]

The formal introduction of DHS in November of 2002, entailed a grant of direct oversight over information analysis and infrastructure protection. Under Section 201 of the DHS Act, the Undersecretary for Under Secretary for Information Analysis and Infrastructure Protection has primary responsibilities for: (1) receiving and analyzing law enforcement information, intelligence, etc. to detect and identify potential threats of terrorism within the United States; (2) assessing vulnerabilities of key resources and critical infrastructures ("KRCI"); (3) integrating relevant intelligence analyses, and vulnerability assessments to identify protective priorities and support protective measures; (4) developing a comprehensive national plan for securing KRCI; (5) taking or seeking to effect necessary measures to protect those KRCI; (6) administering the Homeland Security

[14] *See*, CIAO General Statement of Principals: "in every step and component of the plan, ensure the full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data."

[15] *Carnivore Diagnostic Tool*, Fact Sheet, FEDERAL BUREAU OF INVESTIGATION, *available at* www.fbi.gov/hq/lab/carnivore/carnivore2.htm; *Also see, Internet and Data Interception Capabilities Developed by the FBI Before the U.S. House of Representatives, the Committee on the Judiciary, Subcomm. on the Constitution*, 106th Cong. (2000) *available at* www.fbi.gov/congress/congress00/kerr072400.htm (Statement by Laboratory Division Asst. Dir. Dr. Donald M. Kerr).

[16] *See, e.g., The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age Before the Senate Judiciary Comm.*, Sept. 6, 2000, *available at* www.cdt.org/testimony/000906dempsey.shtml (Testimony of James X. Dempsey).

[17] *See, e.g., National Strategy to Secure Cyberspace*, DEPARTMENT OF HOMELAND SECURITY, July 2002, *available at* www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[18] *Id* at 1.

[19] *Id.*

Advisory System; and (7) review/set policies and procedures governing the sharing of law enforcement, intelligence, etc. relating to homeland security.[20]

Most readers of these guidelines will find them very straightforward and very sensible. The "National Strategy to Secure Cyberspace" addresses five "national priorities": (1) a national cyberspace security response system; (2) a national cyberspace security threat and vulnerability reduction program; (3) a national cyberspace security awareness and training program; (4) securing governments' cyberspace; and (5) national security and international cyberspace security cooperation.

The first priority, response, involves intraspection and analysis of the infrastructure itself.[21] The second priority, reducing threats, introduces an "enhancement" role with law enforcement in the "cyberspace attacks," without a terrorism qualifier, while also addressing many of the issues we have already acknowledged as things that need to be fixed in this system.[22] This includes enhancing the border gateway protocol that routers work on, changing the way the Internet protocol works to provide for more addresses, and better security. To some extent it is a somewhat ambiguous. It contains statements such as "preventing and prosecuting cyber space attacks," "reducing threats," and deterring "malicious actors."[23] My immediate question is this distinction between malicious actor and cyber terrorist intentional? Is this distinction important?

[20] Homeland Security Act of 2002, H.R. 5005, sec. 201.

[21] The National Strategy to Secure Cyberspace RESPONSE (Priority I) agenda includes: 1. Establish a public-private architecture for responding to national-level cyber incidents; 2. Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments; 3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace; 4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security; 5. Improve national incident management; 6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans; 7. Exercise cybersecurity continuity plans for federal systems; and 8. Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.

[22] The National Strategy to Secure Cyberspace REDUCING THREATS (Priority II) agenda includes: 1. Enhance law enforcement's capabilities for preventing and prosecuting cyberspace attacks; 2. Create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities; 3. Secure the mechanisms of the Internet by improving protocols and routing;4. Foster the use of trusted digital control systems/supervisory control and data acquisition systems; 5. Reduce and remediate software vulnerabilities; 6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications; 7. Prioritize federal cybersecurity research and development agendas; and 8. Assess and secure emerging systems.

[23] *See,* Priority II: THREAT AND VULNERABILITY REDUCTION PROGRAM: (1) Reduce threats and deter malicious actors through effective programs to identify and punish them; (2) Identify and remediate those existing vulnerabilities that could create the most damage to critical systems, if exploited; and (3) Develop new systems with less vulnerability and assess emerging technologies for vulnerabilities.

In terms of cyber-crime, America has numerous law enforcement bodies in place, often with overlapping jurisdiction. To the extent DHS starts blending the objective of stopping cyber-terrorism and preventing cyber-crime that is fine. That is a good outcome, so long as it can be done in a way that respects civil rights and the rule of law. The most legitimate argument against Carnivore as a system is that is designed to overstep the Constitutional boundaries of privacy that even the FBI must abide by. To the extent cyber-crime and cyber-terrorism are merged together and DHS will now have jurisdiction and Constitutional flexibility to deal with any suspected cyber-criminal as if they were a potential terrorist, we have a very least some serious challenges. I would say the basic challenges are: (1) the basic issue of the rule of law and civil rights in the context of an expanding security agenda; and (2) acknowledgment that the traditional threats and "malicious actors" are going to continually converge with the DHS agenda. We are going to have a continuing dependence on this infrastructure, and whatever it is we do, we have to remember all that wire. I think it is what, two million miles of cable, something like that?

MS. LUSSENBURG: Oh, it is more than that.

MR. THEOFRASTOUS: O.K., billions. When one speaks of infrastructure today, one has to think in nearly astronomical terms. To the extent we are going to implement change something system-wide, it is going to be very, very logistically complex, and we are going to have to be in a constant training mode. The communication and cooperation internally and externally is going to be something that this Administration is not as good as it might be, at least in terms of a "full duplex" communication.

Consider an example of troubling potential approaches. Look at the website of the Information Awareness Office (IAO),[24] which is a subgroup of the Defense Advanced Research Projects Agency (DARPA). Reviewing the home page for this agency, one can find an explanation of what they do, their mission, and, perhaps surprisingly, limits on their power. That may be due to the fact that if you looked at the home page when it was first rolled out you saw a somewhat menacing kabalistic icon of the "eternal eye" watching the earth. Here is a government agency that is supposed to be making you feel better about what is going on. Obviously, the connotation is that there is an adversary out there now, somebody who is doing things you may not want them to do. The "big brother" behind this perhaps minor faux pas was the initially appointed head of the IAO, John Poindexter, of Iran Contra fame. I cannot say that gave me a lot of comfort.

[24] "The Information Awareness Office (IAO) develops and demonstrates information technologies and systems to counter asymmetric threats useful for preemption, national security warning, and national security decision making." *Mission Statement*, INFORMATION AWARENESS OFFICE, *available at* www.darpa.mil/iao/

In closing, without being overly trite, we have to acknowledge that the strengths of the Internet can all be weaknesses. We have tremendous freedom of access. The market demands that this be an inexpensive, high-performance platform. We will continue to enjoy constant convergence of information technologies and media. And the more the system and its many uses expand, the more it permeates discrete aspects of our work and personal lives. We are increasingly reliant and are thus at risk.

Anti-cyber terror programs are going to have to be, by necessity, extremely complex. They are going to be expensive. We are not talking about largely theatrical measures such as taking away fingernail clippers. We are talking about real systems that have real effect. Few of us in this room will have much information about these systems and their aims, so the political support necessary to drive these initiatives to completion will be an issue. The goals are going to need to be clear. When we look at the issue of anti-terrorism versus law enforcement, we can not accept ill-thought out, vague goals like "monitoring everything." Finally, whatever approach is implemented needs to be creative and sensitive. We must force ourselves to think vigorously about the changes such an ambitious approach to homeland security it is likely to induce on the American public, as well as the rest of the world. This requires us to proceed cautiously and not to jeopardize this critical mission by miscalculating the nature of the threat and appropriate response.