Christopher Boam

Counsel for Internet & Global Ecommerce
MCI, Inc., International Affairs

on behalf of

WITSA

The World Information Technology and Services Alliance

at InfoCom 2003

Panama City, Panama

on June 18, 2003

It's absolutely wonderful to be here at InfoCom. When I was a teenager, a favorite uncle used to regale my brother and me with many stories of the beauty and wonder of Panama. He would talk about the canal, the rich architecture and cultural events – but more importantly about the warmth and vital energy of its people. Indeed, just before he died only a few years ago, far too young, he and my aunt took the last of many trips to this great city. One of the last things he said to me was, "you must go to Panama." I'm proud to say now that I have. And, after only a day in this country's hospitality, it's easy to see why my uncle Joe was so taken.

As Counsel for Internet and Global e-commerce in the International Legal group at MCI, it has been my great privilege to be an active member of the Global Public Policy Committee of the Information Technology Association of America, and its sister organization, WITSA – the World Information Technology Services Alliance. WITSA represents 50 national IT industry associations, collectively representing over 90% of the global market. Among its many functions, WITSA publishes the annual Global Wireless Benchmark and Global Policy Reports, and organizes the biennial World Congress on IT. The topics at-issue for WITSA and the IT industry generally could easily fill a semester of law school. However, the tremendous growth in this region's IT sector presents a great opportunity to focus my remarks this evening on topics very near and dear to me – global trends in legislation affecting the Internet and e-commerce. As the early years of the 21st Century unfold, many have asked a very general question: "What lies ahead for the Internet?" The possibilities are limitless.

Consider that as we sit in this room, there are about 605 million current users of the Internet and as many as 100 million devices on the network. Roughly 33 million of these users reside in Central and South America. However, these figures do not even account for everyday devices like laptops, personal digital assistants and mobile, internet-enabled telephones. Projections of Internet growth suggest that the full range of devices on the Net should be between 900 million and 2 billion by 2006, the latter number if we are to include about a billion Internet-enabled mobile telephones. If present rates of growth continue unabated, by 2010, half the world's population may be able to access the Internet.

Now consider figures for Panama that I found (and many of you may even have better numbers). According to *La Prensa*, an estimated 200,000 people are Internet users in Panama – seven percent of the population – a figure that increases by about 15% per month. Panama's 200,000 amounts to about 6% of all Internet users in Central America, but it's a number that's growing rapidly. Add to this other factors, such as the City of Knowledge Tecnopark in the former Fort Clayton US military base, easy access in Panama to multiple high-bandwidth fiber optic networks, access to active travel routes around the globe and a long history in international banking and service provision, and you begin to grasp the potential. As with any potential, there are not always hard and fast rules for fostering it. But even as we consider the economic growing pains of the IT industry over the past two years, even as we determine internationally how law should keep pace with continued growth in flaccid economic times, we come back to basic questions. What has our experience taught us? Which regulations are worth emulating? Where, dare we say, have we perhaps done it right? And if so, why?

Like many of you, my workday is a mix of both legal and policy facets of many issues that affect the Internet. Most often for me, these issues fall into three somewhat broad categories. They are: cyber-crime and -security, Internet content and related liability issues, and data protection and privacy. As I said recently to a group of students I spoke to in the United States, if you think

it's difficult to negotiate with your parents over which of your brothers and sisters gets to use the car, then you get a sense of how difficult it is to pinpoint what issue will take priority on a given day. But that is the environment we live in. Indeed, for many of us, it marks the key factor why we stay in this business as integral participants in the IT sector – constant change. Isn't it fun? … I can see a few of you chuckling already.

Cyber-crime and Cyber-security

For instance, this "cyber-security" thing - what is it? The answer to that question is deceptively simple. "Cyber-security" represents that combination of both logical and physical technical measures and policy decisions we collectively take to advance the cause of consumer confidence in the Internet. Sounds simple, doesn't it?

Since September 11, the media would have us believe that cyber-crime and cyber-security have *become* the twin watchwords of the Internet. But you know as well as I, that most of the engineers we work with every day have had these as their watchwords for over a decade. In December 2001, a group of international attorneys and engineers met in New York City to weigh-in on the redrafting of a key document that outlines basic benchmarks for global Internet security. The document is the Guidelines for the Security of Information Systems and Networks, prepared by the Organization for Economic Cooperation and Development – the OECD – based in Paris. Now as we sat down in mid-town to re-write, the message was clear. Since 1992, when the Guidelines were first written, a defining change had occurred in the Internet. We had moved from a world of local networks, into one of global open networks. The document had clearly lost its relevance.

The resulting document, approved a remarkably quick seven months later, reflects both the change in networks and some very smart reflection on our world's own post-September 11th fears. The over-arching theme to these new Guidelines is that online participants are becoming more *dependent* on information systems, networks and related services, all of which need – must – be both reliable and secure. Only then can we continue to foster that individual confidence in the Internet so critical to its further development – critical to this tool of both social communication and economic growth. Only an approach that is fully "aware" of its environment – takes due account of the interests of all participants, and the nature of the systems, networks and related services – can truly provide effective security. Thus, within such elements as "risk assessment," "system design and management" and "threat response," the Guidelines emphasize that, as nations look inward to either regulate or advise on implementation of these elements, they must also look outward – to determine the interoperability and compatibility of threat assessment and response. Because the Internet is global, so must be the underlying tenet of any strategy to defend it.

Over the course of several years, I've made it a habit to speak with students about these issues as much as possible – not only because today's students possess the technical abilities that I never had at their age – but also because they are so often on the front-lines in "logical" Internet protection. In fact, the "education" component of the OECD Guidelines was felt to be so vital that both the US Federal Trade Commission and the UK Department of Trade and Industry have embarked on large-scale educational campaigns to develop a "culture of security." Both education programs emphasize not only the *need* to secure home and school systems and

networks, but also to promote *ethical conduct* that recognizes security needs and respects the legitimate interests of others.

One of my favorite questions when I speak to students is this: "Where in the world do you think is the location where the greatest harm can be done on the Internet every day?" I usually follow that question by picking a young person out of the crowd and asking them where they live – "what town?" I ask. Then, I answer my own question by naming their small town as the place where the greatest harm can occur. You can imagine the reactions I get. But I do this only to make very simple points.

Because the Internet has shifted to a global network of interconnected home and office computers, everyone who has a computer and accesses that network has a part to play. And, no one person's role is greater than any other. That means, if you're an Internet user and you use a modem to dial-up and get access, at the minimum, you should have anti-virus software. And, you should set up an account with the maker of the software to have regular virus updates sent to you. Additionally, if the student happens to be among the 13% of Americans who have high-speed Internet access at home – DSL or cable modem – then at a bare minimum, they should also have a smart router and firewall software.

These are precepts that are very basic to you and me. But do our children know about them? Do our regulators, our legislators? I'm proud to say that, little by little, because of efforts like yours – like that of the Software Association of Panama – they are beginning to, but we have much work to do.

One aspect of the debate on cyber-crime that has had tremendous impact, both good and bad, on consumer confidence in the Internet has been use of the Internet for investigatory purposes – data interception, retention and preservation. Each of these methods of retrieving and caching information from the Internet has both proponents and detractors. Without getting too far into the policy debate, but wanting to underscore the issues that both rights organizations and service providers face today – odd bedfellows indeed – let me briefly discuss what we may find in analyzing each of these methods.

First, the technical and cost issues associated with interception. By court order or similar form of due process control, ISPs can be required to perform data interception – the capture and collection of *specific* communications for a *specific* investigative purpose. Traditional interception capabilities employed today were developed to apply to the opening of letters and tapping of telephones. However, the Internet is designed and implemented with a layered architecture of protocols. Depending on the desired information, successful interception requires capture and interpretation of multiple layers of protocol.

Moreover, data flows in the network are dynamically routed so that interception must occur close to either source or destination in order to have a chance at capturing all that might be of interest. Interception in the middle of the network is unlikely to produce the desired result. Thus, if it's the desire of authorities to retrieve the "content" of an email transmission, it requires complex equipment, positioned in the right place, at the right time and in the right way. And we haven't even touched upon whether the content has to be cryptanalyzed for content or if the email sender has "spoofed" their return address.

But perhaps of even greater impact than the technical issues associated with existing interception legislation is blindness to bottom-line realities. Service providers should not alone bear the cost of assisting law enforcement in combating computer-related crime. Any proposed legislation should include provision for reimbursement of costs involved with data interception or other activities mandated by order of law enforcement. Without a mechanism for facilities and equipment reimbursement, the cost burden of complex search and seizure requirements could put smaller service providers at substantial financial risk. Additionally, there will be a resulting opportunity cost in having to divert resources and technical expertise from further development and improvement of services. This, in turn, leads to both higher cost Internet services and decreased availability of innovative services to the public.

For instance, the lawful interception acts of the Netherlands, Belgium and South Africa all require that service providers not only create or obtain the necessary equipment to facilitate interception upon law enforcement request, but they must acquire this capability and utilize it on a case-by-case basis all without opportunity for compensation by authorities. The resulting costs in the Netherlands, for example, can equal as much as 1.2 million US dollars initially and many thousands annually, depending on the size of the service provider. By contrast, the US Patriot Act of 2001 and Australia's lawful interception act each provide for law enforcement's provision of the equipment and reimbursement to the service provider for manpower and technical costs associated with the handover of intercepted material for specific requests.

Reimbursement would also serve to safeguard the privacy rights of individuals. If law enforcement agencies are held accountable for the costs of interception and investigation, it is likely that they will be deterred from abusing investigative requests, seeking over-inclusive requests or targeting individuals inappropriately. The protection of industry and fundamental human rights are uniquely linked in this instance.

Service providers have a stake in assisting law enforcement to keep the Internet a secure place to conduct business. However, without the pertinent detail and authority of a clear court order, Internet users would be subjected to surveillance of their communications based upon varying levels of substantiation, further eroding consumer confidence in the Internet. It is for this reason that policy makers in the US, Great Britain and Australia have taken particular pains to debate the quality and specificity of substantiation necessary for an intercept order in an Internet environment. Without a court order, service providers would also expose themselves to potential liability for the results of interception requests, whether legitimate or not. To this end, key components of a balance with investigative aims must be the twin goals of due process for end users and immunity for intermediaries that follow the instructions of law enforcement

Of course, fundamental to this investigatory debate is *storage* of this information once it is retrieved. Data "preservation" is most nearly like a traditional wiretap, where authorities require a service provider by court order to retain all communications but only for a *specific* individual and for a *finite* period specified in the order. This is the investigatory storage scheme in place in the US, Australia and several other countries. Service providers have a strong track record of working closely with law enforcement under national statutory arrangements. In fact, this cooperation often includes real time interception of communications and the preservation of traffic data that are routinely collected for legitimate business purposes. Because data preservation targets a specific individual for interception or monitoring of their communications – and for a finite period of time specified in the order – cost implications are minimized and

rights consequences are brought within the margins of due process protections. The probability that a crime or violation is occurring is known, and the investigation limits clear.

In stark contrast, data "retention" is the collection of *all* data traversing the network, regardless of sender, recipient or investigative purpose, for eventual review by authorities as need *arises*. Data retention proposals vary according to the length of time for which data will be retained and whether the data retained will include just "traffic" information (sender/recipient, header or subject line and file size) or full content of a communication as well. Whereas many have recognized that data preservation regimes are entirely satisfactory for most occasions when law enforcement requires information from service providers, many governments – particularly in the European Union – appear to be favoring implementation of mandatory retention.

Of great concern is the variance and length of the proposed retention periods, which have ranged from 3 months to an improbable 3 years. The lack of consistency in storage periods will be a significant additional burden on service providers operating in multiple jurisdictions. But of even greater impact will be the lengths of time required, for here are the cardinal principles. The cost to both store and search data stored from a network increases exponentially over time. And importantly, the ability to effectively search that retained bulk data for whatever law enforcement might be looking for decreases exponentially over the same period. Consider, for instance, that roughly 40 percent of most Internet traffic consists of spam – and that this material would be retained as well – and you get a perspective on the potential storage and search problems. It will be costly and serve little investigative utility, other than perhaps a legislator's piece of mind.

The possibilities for retained data misuse are significant. But surprisingly, some parties have begun using the debate over retention to promote other possible – though dubious – end uses for retained data. Those countries that have already imposed mandatory data retention regimes, including Switzerland, Austria and Belgium, require that the data be accessible only to law enforcement and solely for the purpose of criminal investigations. Indeed, none of the present proposals for mandatory retention even hint at providing access for private rights of action. However, this has not deterred some in the content community from suggesting that retained data – once service providers have been required to store it – should be used to investigate possible copyright infringements by end-users. For this reason, some have been odd proponents of an investigative requirement with enormous costs, risks and rights implications.

The basic starting point for any discussion on the investigatory aspects of cyber-crime legislation is the need for a harmonized approach to prevent a patchwork of laws that will balkanize the global Internet. Purely national standards for lawful interception are difficult to maintain, problematic to implement and are frequently not supported by manufacturers of the necessary equipment. At a minimum, any proposed legislation on computer-related crime should be *consistent* with existing law and with developing international standards. Consistency is key to avoid impeding the delivery of innovative e-commerce services, while at the same time protecting consumer confidence in the medium.

However, key to determining the appropriateness of interception standards and the use of preservation or retention regimes, are three very important questions. First, what information do authorities hope to retrieve? Second, what authority or process is necessary for service providers to comply with law enforcement requests? And third, what is the impact of the method on

individual rights and the economic viability of service provision, and how does this impact balance with both the need for the information and the potential for its successful retrieval?

There are ways in which interception and preservation can serve law enforcement needs while safeguarding the economic viability of and consumer confidence in the Internet. Through understanding of the technology involved, what it costs and how it is effective, legislation can be crafted to serve the greater good. Of the three concepts discussed, data retention meets none of these tests, and indeed, could ultimately do greater harm than provide law enforcement value.

Content Liability

Several aspects of the cyber-crime / cyber-security debate touch upon issues of technical infeasibility – the inability of the Internet to act or do what some would like it to do. Perhaps none of the issues relating to crime and the Internet is impacted more by technical infeasibility than the issue of content liability.

Presently, there exist mechanisms for "notice and takedown" – for service providers to be notified of content that should be removed. The US Digital Millennium Copyright Act (DMCA) includes a notice and takedown provision (sanctioning ISPs to act on notice, as opposed to proactively), and the EU Copyright Directive similarly minimizes service provider liability if they act as a mere conduit (transmission without 'positive knowledge' of infringing material). However, some content providers are attempting to re-open the debate, seeking ISP obligations to proactively monitor networks for infringing content and assume a greater share of liability.

The burdens associated with a proactive monitoring requirement would be devastating, from a legal and economic perspective. Service providers need a clear legal procedure (*i.e.*, notice & takedown) to avoid liability to any potentially infringing customer. Further, proactive monitoring of Internet networks – if at all feasible – would lead to higher costs necessitating network design changes and significant human resource allocation. The service provider industry as a whole has attempted to deflect further legislation by sticking to what has been a carefully balanced compromise. The EU Copyright and E-commerce directives, and the US DMCA, reflect the achievement of a delicate balance between the different interests of all stakeholders involved in e-commerce transactions.

Not long ago, Internet service provider UUNet received a threatening e-mail letter asserting that one of its customers had violated a Warner Brothers copyright by downloading the film "Harry Potter and the Sorcerer's Stone." Coming as it did in the midst of the content industry's heightened crusade against the illegal swapping of songs and movies, the letter demanded drastic remedies. Warner Brothers wanted UUNet, a subsidiary of MCI, to cut off Internet access and terminate the account of the suspected infringer. But there, the studio's case quickly unraveled. The file carried the .rtf suffix, meaning it was a Word file and not moving pictures, which usually carry the .mpeg or .mov suffixes. The file was also less than one-millionth the size of a normal digital recording of an entire movie. And then there was the file's full name – "harry potter book report.rtf." Recognizing they were dealing with a school project, instead of a pirated movie, officials at UUNet ignored the studio's demands. Entertainment companies say wrongful accusations, such as in the Harry Potter case, will be a rare but necessary byproduct of a hunt for Internet copyright pirates that are costing the industry hundreds of millions of dollars a year.

However, this hunt has now taken on grander dimensions than just letters. Under the DMCA's Section 512(h), subpoena power is granted to copyright holders. But this power had never been given unrestrained interpretation until a judge's ruling in the US last month against Verizon, which will force administrators of local college networks and service providers to turn over the names of service subscribers if copyright holders want them. The judge rejected Verizon's arguments that the DMCA does not permit such a violation of due process and free speech. As a result, Internet users who *may* have illegally downloaded copyrighted songs or movies may suddenly find out this fall that their service provider cut off their Internet access and gave their name, address and phone number to entertainment industry lawyers. And this can happen all without the service provider having the ability to determine whether or not the content industry's allegation has any merit.

Service providers generally support the aim of effective intellectual property rights enforcement, as these companies all own a wide range of intellectual property rights. The establishment of appropriate conditions for the creation, distribution and use of digital content is crucial and depends, to a large extent, on effective IPR protection and enforcement. However, such laws should not be enforced without due process. By allowing copyright holders to obtain the names of Internet users without a judicial determination that a user is likely engaged in illegal conduct, we will be permitting virtual "witch hunts" for defendants presenting the worst facts or having profiles least likely to garner public or judicial sympathy. Even worse is the prospect that anyone *claiming* to be a copyright owner could now have the scarcely constrained right to obtain identifying information about any Internet user. Even where laws exist, there must be constraints to the enforcement process and judicial oversight or there will be a grave risk of abuse.

In 2002, service providers also faced orders from national authorities to block access to content regarded either as harmful or illegal – for instance, Nazi-related content barred in Germany and France. The problem in most of these situations is two-fold. First, the relevant content is frequently hosted outside the jurisdiction of the country where the order appears. And second, the service provider subject to the order does often not host the content.

Blocking access to specific material that a service provider itself doesn't house is often not technically feasible, and it is nearly always improbable to limit an attempted block to subscribers of a particular geographic area. It is for this reason that the Panamanian high court last November suspended an order that ISPs block 24 UDP ports targeted as likely used to carry voice-over-the-Internet (VOIP) traffic. Despite that the ports targeted were necessary to other types of communications that neither begin nor end in Panama, most VOIP applications utilize far more than the 24 ports listed in the suspended resolution, and further, could quickly bypass the 24 blocked ports. As a friend recently said to me, by analogy, "if you're a policeman, and you want to catch speeders, you don't install policia morto every ten feet (speed bumps) to slow down all the traffic."

Internet networks do not recognize geographic boundaries. Moreover, users located in one geographic area can access the Internet by accessing network connections in another geographic area. Further, even if forced to attempt a "block," service providers cannot block access to certain Web sites on the Internet that they do not host without blocking access to other, completely unrelated, *legal* content. All the while, the alleged illicit site can simply change its location to avoid the attempted block.

Legislation and regional codes of practice on these topics often fail to embody three key components with regard to the liability of a hosting (or non-hosting) service provider:

- First, there must be recognition of the fact that a service provider that does not host the alleged illicit content has little if any effective technical ability to block it. And forcing an ISP to attempt a block can often exacerbate the problem.
- When a service provider does host material found to be illicit, there needs to be a process by which *law enforcement* makes the determination as to what is "illegal," etc., based upon a legal or regulatory scheme that defines such material.
- And finally, there must be formal adherence to due process by law enforcement in requiring ISPs to remove designated material in order to limit liability for acting in accordance with the order.

Service providers share the abhorrence of illicit online content such as child pornography and are proud of extensive efforts in cooperation with law enforcement agencies that are investigating and prosecuting those responsible. Law enforcement and local non-hosting service providers can most effectively and efficiently combat illicit content by identifying the service provider that has the ability to remove the content in question at its source.

Meeting last month in Strasbourg, the Council of Europe's Council of Ministers adopted a declaration on "Freedom of Communication on the Internet," striking a high-level but much needed balance among several key issues potentially affecting open Internet communications and the provision of Internet-based services. Although not "all things to all Internet stakeholders," the declaration represents the best and most balanced high-level position on these issues we've seen for some time. The declaration urges member states:

1. To refrain from subjecting online content to tougher restrictions than those imposed on other means of content delivery.
2. To encourage self- or co-regulation of Internet content.
3. Not to block or filter content or deny public access to it, with the exception of filters aimed at protecting children.
4. To encourage universal access to Internet communications and information services on a nondiscriminatory basis at reasonable cost.
5. Not to subject the provision of online services to special authorization schemes solely on the ground of the means of transmission used.
6. Not to hold ISPs liable for Internet content when they merely transmitted information or provided access. However, the CoE said, ISPs could be held co-responsible if they didn't take down sites when they became aware of their illegal nature.
7. To respect the decision of users to remain anonymous online.

Data Protection and Privacy Self-help

Several of the issues I've talked about this evening can potentially conflict with principles of personal privacy online. Indeed, since 1995, the issue of online privacy has developed from a discussion involving mostly lawyers to a key concern of most Internet users. Since the European Union adopted its Data Protection Directive in 1995, many other countries have followed suit.

Argentina and Brazil have enacted Habeas Data laws, Mexico most recently introduced the Torres Bill – which mirrored Spanish legislation, Japan passed data privacy legislation only last month and India is poised to do the same in the very near future.

Each of these laws, and those in the United States, share similarities in that they all serve to protect against misuse of personal information. But indeed, many of them differ in scope, which poses enormous difficulties for international businesses hoping to comply. Whereas laws modeled after the European Union's privacy regime apply equally to all aspects of "personal information" both on- and off-line and across industry sectors, many laws – including those in the United States – apply protections that are weighted according to the potential for misuse of certain personal information, and these protections are in turn applied sectorally – to the healthcare industry, the financial services industry, and so on. Some have argued that the "omnibus" protections of Europe's Data Protection Directive are too restrictive. Further, many have complained that member states of the European Union can "gold-plate" these protections at the national level, making cross-border compliance a nightmare of complexity. In turn, others may have a valid argument that the sectoral protections of the US are simply insufficient to guarantee the basic privacy rights of those online.

This is debate that could consume a whole conference in itself, and has. So instead of debating the merits of different systems, let me leave you with a few key precepts. As countries revisit existing privacy laws, either to strengthen protections or seek to have existing protections apply online, there are four key principles that should help guide the debate:

- ***Relevant Risks*** – Create rules that focus on the risk attributable to misuse of certain types of data in setting the level of protection for that data;
- ***Consistent Implementation*** – Ensure that national legislation cannot embellish regional framework or other international DP requirements with added protections that frustrate the possibility of cross-border compliance;
- ***Flexible Compliance Options*** – Enable regulatory authorities to review and give the "stamp of approval" to appropriate industry and NGO-developed compliance contracts, codes and procedures; and
- ***Consultation*** – Industry understands that its role in DP compliance supports its mission to achieve and retain customers, and thus, industry consultation at all levels of DP legislative development will improve compliance and enforcement.

The second set of precepts I want to leave you with concerns what I like to refer to as the "privacy gap" (nothing to do with the clothing retailer). No matter where you live and what privacy protections are in place in your country, there will always be an element of self-help necessary to protect your privacy online. The law cannot do it all for you, and as they say in London when you board the subway system, "mind the gap." When I spoke recently to a group of students in the US, I asked them to compose their own set of top four online privacy principles, and I must say that they did an outstanding job. So here they are:

- Number 4: ***Ask questions*** – Before you give a Web site your email address, phone number, home address, check out their privacy policy or email them a question. If you don't get a good answer, move on.

- Number 3: ***Protect yourself from Harvesters*** – People that want to send you spam will look for your email address anywhere and everywhere. Consider creating a "disposable" email address to use in public postings, online purchases and online chatting.
- Number 2: ***When it comes to Spam, don't talk to strangers*** – Which means, if you get spam, and you've never heard of the company or sender, don't waste your time sending them an email to take you off their list. Unfortunately, 9 times out of 10, they're simply hoping you respond so that they can see your address is "live" and send you more Spam.
- Number 1: ***Never ever use a social security or government ID number online*** – Many US states have laws prohibiting companies from asking for your federal ID number, and many other states are considering laws. But most reputable online companies both in the US and abroad will never ask you for it, and if they do, they'll give you several other options for you to identify yourself. You don't want that number misused, online or anywhere else, so don't use it – period. If somebody online says you need to use it, then take your business elsewhere.

Closing

We can already sense the effect that global communication and interaction among individuals is having. Unlike the telephone, the Internet allows groups of people to discover and interact with one another on the basis of common interest. One need not know who the other parties are before interacting with them. Media such as television, radio, newspapers and magazines allow a *form* of group interaction, but it is point-to-multipoint and largely one-way. The Internet facilitates interactions among parties and the sharing of information in ways that are wholly new. The sharing of knowledge and indexing of its content, however crude these indexes may be, has transformed the way in which research is conducted, the way commerce is transacted and the way buying and selling can be effected. An auction involving millions of participants is no longer unthinkable. It is a daily occurrence.

It is not enough to fashion legislation or to establish practices that are purely local or even national in scope. Whether you are considering cyber-security, content liability or privacy legislation, the border-crossing Internet guarantees that virtually any activity conducted through the network can be undertaken locally, nationally or internationally without much if any, visible difference. Legislators will be challenged to develop and pass laws that "inter-work" at national or other geo-political boundaries, for if there are gross disparities, there are sure to be distortions in international commerce and user behavior on the network. For instance, the challenges of inter-working and digital signatures in contracting were marvelously begun here in Panama in 2001 with the passage of the E-commerce Act, the first of its kind in the region. And I know that you have next steps ahead in that process.

But beyond considering the proportionality and interoperability of legislation, remember that there must always be a personal element. I've always wanted to be a lawyer, but the thing I love most about what I do is that, ultimately, the success or failure of it depends on everyday people making everyday choices in a world that has grown much smaller in size. The common element in all legislation that affects the Internet should be the interests of ordinary people as end-users, whether that's you and me with our high-speed lines, or those for whom Internet cafes represent their access to a brave new world. The power of our choices in that decision-making, how they're molded, how they're exercised, is something that will ultimately shape all of our lives.

There's an old speech-making trick that illustrates the power of our individual relationships and how they shape what we do in business. You take a glass jar and fill it with golf-balls. With golf balls to the top of the jar, you ask the audience, "is the jar full?" The answer is, "no." So then, you take pebbles – little stones – and fill the jar around the golf balls until the stones reach the top. Is the jar now full? "Not yet," is the reply. Next you add sand, and then improbably, a can of beer, before you can truly say that the jar is "full." But what does this represent? Well, the golf balls represent our relationships with family, loved ones and friends. By not adding them to the jar first, we can neither add them later nor hope to truly fill the jar after we add the little "pebbles" of training and the "sand" of experience. Nor would that beer at the end of an accomplished day taste quite as good.

In our interconnected world, at no other time in our history are your choices more meaningful – each and every one … on the Internet and beyond. As a family, discuss what is and is not appropriate to view or do on the Internet. But most of all, remember that the Internet is only a tool. Occasionally, just choose to turn it off. It's the measure of a country's history and freedoms that some things be protected speech, no matter how objectionable we might individually feel they are. But it's the measure of a family, community, of a regulator, and how we personally communicate, that impacts individual choice and makes us uniquely responsible users of the Internet as the first true window on the world. As citizens of an interconnected world, you will be inspired by what you learn and by the people around you, whether you realize it or not. Remember to look for inspiration in the simple as well as in the profound. Thank you for the honor of speaking to you this evening and enjoy the next two days of InfoCom 2003.

About the speaker: Christopher Boam is Counsel for Internet and Global E-commerce in MCI's International Affairs division based in Washington, DC. His primary duties involve both legal and policy-related facets of data protection, cyber-crime and -security, broadband development and related Internet content issues. He is also an active member of the Global Public Policy Committee to the Information Technology Association of America (ITAA), providing consult and input to the World Information Technology and Services Alliance (WITSA). Prior to joining MCI in 2001, Mr. Boam served in both Member office and Committee staff positions in the U.S. House of Representatives and in private legal practice with a US-based firm. He is a graduate of the University of Scranton, in Pennsylvania, and the Catholic University of America Law School, in Washington, DC, where he served as Editor-in-Chief of the Communications Law Review. Mr. Boam has published over a dozen articles and monographs on issues relating to Internet regulation, in such publications as the *Journal of Communications Law & Policy*, *Hastings Journal of Communications and Entertainment Law*, *National Law Journal* and the *World Intellectual Property Law Journal*.

About WITSA: The World Information Technology and Services Alliance (WITSA) is a consortium of 49 information technology (IT) industry associations from economies around the world. WITSA members represent over 90 percent of the world IT market. As the global voice of the IT industry, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including:

- *increasing competition* through open markets and regulatory reform;
- protecting *intellectual property*;
- encouraging cross-industry and government cooperation to enhance *information security*;
- bridging the education and *skills gap*
- *reducing tariff and non-tariff trade barriers* to IT goods and services; and
- safeguarding the viability and continued growth of the *Internet* and *electronic commerce*.

Founded in 1978, WITSA has strengthened the IT industry at large by promoting a level playing field and by voicing the concerns of the international IT community in multilateral organizations, including the World Trade Organization (WTO), the Organization for Economic Cooperation and Development, the G-8 and other international fora where policies affecting industry interests are developed.

About MCI: With more than 20 million business and residential customers, MCI® is a leader in serving global businesses, government offices and U.S. residential customers. MCI delivers a comprehensive portfolio of local-to-global business data, Internet and voice services to a 'Who's Who' list of the Fortune 1000. Our portfolio includes SONET private line, frame relay, ATM and a full range of dedicated, dial and value-added Internet services. MCI today owns and operates some of the world's most complex and sophisticated custom networks, and is an established leader in IP network technology and Virtual Private Networking (VPN), delivering VPNs based on private data networks as well as our global Internet backbone, which spans six continents. We also are a premier provider of audio, video, and Net conferencing services that enable customers to meet and collaborate remotely to effectively conduct business anywhere, anytime.