WEEKLY MEDIA BRIEFING WITH ATTORNEY GENERAL JANET RENO

AND WILLIAM M. DALEY THURSDAY, MARCH 9, 2000

SECRETARY, U.S. DEPARTMENT OF COMMERCE

SUBJECTS: REPORT OF PRESIDENT'S WORKING GROUP UNLAWFUL INTERNET CONDUCT

ADDITIONAL SPEAKER: JOHN RYAN, ASST. GENERAL COUNSEL, AMERICA ONLINE

U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

THURSDAY, MARCH 9, 2000

9:31 A.M. EST

ATTY GEN. RENO: Good morning.

I am joined today by Secretary of Commerce William Daley and assistant general counsel of America Online John Ryan to talk about the report of the president's working group on unlawful conduct on the Internet.

In August of 1999, President Clinton asked me to chair an interagency working group to analyze the legal and policy issues created by unlawful conduct on the Internet. Today the working group, with industry support, is issuing its report.

The Internet has provided our world with unparalleled opportunities, many of which we are just discovering and probably many yet to come. At the same time, the Internet is providing criminals a vast inexpensive and potentially anonymous way to commit crime. How we respond to these challenges posed to law enforcement will be critical

to public confidence in this

wonderful medium. Our working group analyzed this potential for criminal behavior and reached three conclusions:

- First, existing laws in the physical world that apply to illegal activities, such as fraud and possession of child pornography, should apply equally on the Internet. That means we can, and we should, use existing laws to prosecute most unlawful conduct on the Internet. And we must ensure that regulation of unlawful conduct on the Internet is treated in the same manner as off-line conduct, is technology-neutral, and is handled in a manner that takes account of other very important interests, such as individual privacy.

- Secondly, law enforcement faces significant investigatory and procedural challenges in combatting unlawful conduct on the Internet.

  These challenges include the inability to trace criminals who hide their identities online, difficulty in finding criminals who might be located in other jurisdictions, the need for better coordination among law enforcement agencies, and the need for trained personnel at all levels of law enforcement.

  In addition, the working group identified several areas where legal authorities and tools needed to combat cybercrime are insufficient. We recommend that the laws relating to the investigation and prosecution of high-tech crimes be evaluated, to ensure that they keep pace with technological and social changes.

- Third, there should be continued support for private-sector leadership, to promote cyberethics, to minimize the risk of unlawful activities on the Internet.

These interests, if addressed properly, are not inconsistent, but they are mutually reinforcing. And they can result in consumer confidence, ensuring that the Internet is a safe and secure medium for facilitating commerce, expanding communications too, and bringing countless benefits to our lives.

The Federal Trade Commission, the Department of Treasury, and other agencies have been vital partners in this effort, and I want to thank them.

And now it is my pleasure to ask Secretary Daley to discuss his thoughts on the report.

SEC. DALEY: Thank you very much, General. And Mr. Ryan, thank you for having us here together for the issuance of this report.

When we began preparing the report, the issue before all of us was whether our existing laws were adequate to protect online activities. I think the report concludes that in most cases our laws do work. So the issue has become whether law enforcement has the tools and resources and also the proper training to fight new criminal behavior. Obviously, the attorney general feels that we do need more resources. And just as importantly, we need to figure out how to give law enforcement the tools in a way that is not harmful to the Internet and obviously not intrusive to business. We absolutely have a need to do this right.

As we have said many times, if e-commerce is to meet its potential, people must trust the Internet, or they will be reluctant to continue to do business over the Internet. We've spent a great deal of time working on privacy and consumer protection concerns, but to be frank with each other, what is an even more basic concern to consumers is the issue of security.

In my opinion, businesses must step up their own efforts to make the Internet more secure and not wait for cybercops to be expanded. After all, networks are in the hands of the private sector. It is the private sector that has made the most progress of information technologies, and there are things, as the report concludes, which businesses can do to make the Internet safer.

Let me just highlight three of them.

First, businesses should continue to develop initiatives to protect consumers and children online. Companies have developed technologies that block things that none of us would want our young children to see. Many organizations have developed educational programs aimed at instructing younger Internet users about online citizenship. There

are programs that advise parents in how to protect their children online, and we need to see more of these activities.

Second, businesses need to cooperate with law enforcement agencies more often. We are not asking businesses to be online cops, but we want them to be online Neighborhood Watch groups. They can do for the Internet what neighbors do for each other in every community of our country. That is, making their community safer by keeping an eye on each other. I think they should share their experiences and technologies with law enforcement. This is not easy, and there will obviously be concerns about protecting proprietary information.

Well, one of the major reasons for our success in addressing the Y2K problem is that industry and government came together and made it work. I think if companies can help nail hackers who threaten our networks, it's not just good in fighting crime, but it is good for the future of e-commerce. A number of e-businesses have developed channels of communications with law enforcement of efficient procedures to process their requests. They have also been educating their employees about how to recognize unlawful conduct on the Internet. These practices should become standard operating procedures for all businesses who do business online.

Finally, let me say that in 1997, President Clinton and Vice President Gore made the right choice when they came out for the first policies on e-commerce, and that first policy was that the private sector should lead. Some things, obviously, deserve protection as a matter of law, but one reason the Internet has been so successful is that government has avoided regulation that would have messed things up. The Internet and e-commerce are changing so quickly, we must continue to work together, employing all of our talents and experiences to ensure its successful and continuing growth.

This report sets an agenda of issues that we must address together as the Internet grows even more important in each of our lives, important not only for business, but for education, communication and entertainment.

So we look forward to working with the attorney general and the private sector to find ways to implement these recommendations.

Thank you, Janet.

ATTY GEN. RENO: Thank you.

Q Mr. Ryan, what about the issue of anonymity? How important is that to Internet service providers? And should there be some way that law enforcement can penetrate the anonymity for anyone who uses the Internet?

MR. RYAN: Well first, let me preface my remarks by stating that, on behalf of America Online and my industry colleagues from the Internet Alliance and the Information Technology Association of America --

Q (Inaudible) -- pardon me. Could you --

MR. RYAN: Yeah?

Q -- lean forward so --

MR. RYAN: Yes, sir.

Q -- the camera can see you?

MR. RYAN: The industry would like to commend and thank the efforts of the entire working group, in particular the agencies, the Department of Justice and Department of Commerce, in the thoughtful and comprehensive treatment that is reflected in this report.

As this report indicates, this report is not meant to offer specific recommendations but rather a framework to continue the dialogue between the existing partnership that exists between private industry and the governmental agencies that have an interest in promoting a safe and secure experience.

Anonymity is one of the issues that this report deals with. But it specifically leaves to further dialogue a more comprehensive and thoughtful discussion of how to balance the privacy interests of those who use the interactive service, as well as those who seek to abuse it. So rather than deal with specific comments on the issue of anonymity, I think we are prepared today to commit ourselves to continue with this dialogue, between industry and the public safety, to make sure that all the important issues that are raised in this report are dealt with.

Q Well, speaking of dialogue, what is -- just to engage in a little here -- what is the industry's view about anonymity?

Should it be preserved on the Internet? Or should there be a way for law enforcement, with proper court orders or subpoenas, or whatever, to pierce that anonymity, if they feel they need to?

MR. RYAN: First, this report reflects that there are existing statutes, notably the Electronic Communications Privacy Act, that sets forth the guidelines that exist, whenever law enforcement seeks to acquire information or data from an Internet service provider or a member who uses that service.

So there are existing guidelines that safeguard both the privacy interest and the legitimate needs of law enforcement when they need to investigate instance of abuse.

So we are not looking -- and we commend this report for not looking to create necessarily new laws. We point to existing safeguards that promote both public safety concerns as well as the privacy interest.

Q Ms. Reno, on the --

Q One more on this subject: Does the industry collect the data necessary to answer those questions when law enforcement comes knocking? Is the industry pretty good about collecting at some point information on who is using generic names on the Internet?

MR. RYAN: You must recognize that there are different business models that are involved in terms of those entities who engage in business on the Internet. There is no single business model that is engaged in or adopted by all the various entities.

So that question is left to each individual company to serve the interests of their subscribers, as well as whatever is the best business model.

Q Ms. Reno, when the National Infrastructure Protection Center was established a couple years ago, as I recall, you and Mike Vatis talked about particular investigative and prosecutorial guidelines for this brave new world, similar to the department guidelines that

it uses in the physical world. Were these guidelines peculiar to the Internet or peculiar to cyberspace ever developed, or --

ATTY GEN. RENO: We're in the process of trying to figure out what guidelines should apply. As I have mentioned to you and as we have discussed with industry, we're going to be having a conference -- hopefully one on the West Coast and one on the East Coast -- with the industry and others who are concerned, to hear from them about what we can and can't do, should and should not do, and how we can develop the partnership with industry that is so vital. I don't want to put anything in stone until I make sure that I have heard from everybody concerned.

Q Ms. Reno, you used the term "cyberethics." What are they, and who determines the standards for -- the ethical standards here?

ATTY GEN. RENO: I don't mean to be repetitious, but I think the best description was from the gentleman who knows an awful lot about cybertechnology, pointed out to me that his 13-year-old daughter knew not to open other people's mail, not to go in somebody else's room and rummage through their desk, but he wasn't sure that she knew what to do not to do on the Internet.

And it is to carry forward our ethics of the physical world into the Internet, so that people can have an understanding of, "You don't do this, you can do this, this is permissible, you'd better watch out if you do this."

Q Ms. Reno, pornography taints the Internet, and I would ask Secretary Daley to ask what kind of measures -- are there active measures to take down this porn? We know that there are measures to protect children and, you know, household users, but what would -- what would you recommend to Ms. Reno and vice versa on this particular matter?

SEC. DALEY: Well, I wouldn't be recommending any legislation or action. Obviously, if criminal activity is going on around pornography using, whether it's the Internet or non-Internet, law enforcement has a legitimate right to take action as they do and as they do often. But what we have spent three years doing is encouraging industry -- and they have moved very aggressively to create the technologies so that people can protect their children,

and those adults who want to engage in those activities that are legal, they have every right in the world to do that, and n o one is talking about taking action in that area.

But industry has stepped up, and it was a result of a significant movement by not only the political establishment, but by normal people out in America in response to -- at the beginning, even in the first year, three years ago, that I was engaged in these issues as secretary, like 80 percent of all comment about the Internet in media was about pornography, and about the explosion of that. That's not written about much any more, and I think that's a combination of, one, real technologies have been developed that parents are taking advantage of so that their concerns of a few years ago have been addressed, and at the same time, the explosion in so many other areas of the Internet that have overwhelmed that small piece of the Internet that was so prominent a mere three years ago.

Q Do you feel that there is a legitimate place for pornography on the Internet?

SEC. DALEY: Well, the courts have said there's a legitimate place for those activities in our society, as long as they're within the confines of the law, whether it's on the Internet or off the Internet.

ATTY GEN. RENO: I think the report's basis is existing laws in the physical world that apply to illegal activities, should apply on the Internet. And it is clear that we have put a lot of time and effort into child pornography on the Internet, through the Innocent Images Program, and otherwise. But that is the basis of this report. It doesn't pass judgment on the physical world; but it says, "If it applies in the physical world, it should apply on the Internet."

Q Let me just make one clarification. So does this report -- or are you advocating any new laws that would be even stronger than -- (inaudible) -- or simply proper enforcement of existing laws on the Internet?

ATTY GEN. RENO: What we are talking about is let's use, substantively, the laws that exist in the physical world and apply them to the Internet, and let's be technology-neutral. But let us recognize that there are investigatory steps that may need to be

taken to effect the same result as in the physical world:

Let us discuss those. Let us understand what the balances are. Let us sit down with industry. Let us hear from the privacy groups. And let us see how we balance the interests, which exist day in and day out, for all of law enforcement: When can you take action and when can't you?

Q So it's really more -- to the extent that you'd need improvements in the laws, it would be in the procedural type elements of the law --

ATTY GEN. RENO: Yes.

Q -- for example, how to do trace work and that sort of thing -- multijurisdictional law and that sort of thing?

ATTY GEN. RENO: I mean, we have talked about it before. If a man can sit someplace halfway around the world and steal from a bank in the United States on his computer, we are going to have to develop new ways of processing these cases -- of working with our colleagues around the world, of bringing these people to justice.

Q May I ask about how you might apply your thinking to two specific problems that would seem to me very important for investor and consumer confidence in the growing e-commerce world?

Specifically, we have seen some things in the news lately about people who hack into e-commerce sites and steal credit-card numbers and billing information, and also people who overload e-commerce sites and essentially sabotage them.

Those would seem like key things that could really hurt the growth of this segment of the economy. What specific changes do you folks want to see to better prevent that types of sabotage, in fact?

ATTY GEN. RENO: I don't want to make specific proposals. What I want to do is to sit down with industry, with the privacy sector, and figure out how we deal with those issues. If a man masks his identity, as he takes the credit-card numbers and other identifying information and invades the privacy of everybody in this room, everybody in this room is going to want to know who got their credit-

card number; who is using it, who is extorting them -- whatever he is doing with it.

How do we balance that with the need for people to be able to use the Net in a private way? Those are the issues. They are not easy issues, but I think we're trying to effect a discussion that can help us understand it.

Now, the best way to understand something is to not deal in "what ifs" but to come up against the hard questions. And what happens if you have somebody who's threatening to open a massive dam and let water flow out that would cause tremendous damage; he's masked his identity -- what should law enforcement be able to do in those circumstances? What capacity should it have to identify him, other than through activities normal to law enforcement in the physical world? These are the issues, and this is what the report indicates we need to resolve.

Q In terms of --

Q Ms. Reno --

Q Can I just follow up? In terms of the time line, how do you balance the need to think these things out well with the fact that right now we are in what could be a key growth phase for this industry? A lot of companies are forming, they need capital, consumers are just shifting in here. The more you see things in the news about credit cards being stolen or sites being shut down, the harder it is to start up in this sort of key growth phase.

ATTY GEN. RENO: I think Francis Thompson had the best line: You do it with all "deliberate speed" and "majestic instancy." (Scattered laughter.)

Q Madame Attorney General, last September the administration announced a change in its position with regard to the export of strong encryption. Could you comment on how that change in policy will make the Department of Justice's life more difficult with respect to tracking anonymous use of the Internet?

ATTY GEN. RENO: I think we are going to be able to address the issues, particularly as we form strong partnerships with industry,

recognizing that industry should be involved, as the secretary has indicated, in developing processes and procedures that protect itself and the Internet from abuse, and recognizing that law enforcement, working with industry and having access to industrial knowledge, can do so much in terms of avoiding the encryption and getting to the wrongdoer.

Q Ms. Reno, is it sort of extraordinary that it would -- that one of the conclusions that you have is that the law should apply to the Internet as it does everywhere else? Why is it even necessary to say that? And is there -- is part of the answer to that that there's been a sort of culture developed about the Internet that it's different, it's apart, should be hands-off?

ATTY GEN. RENO: I think it's been developed -- and the secretary and Mr. Ryan might want to comment -- because law enforcement got into it and said, "Oh, we need this and this and this," not recognizing that here is a new tool that, if properly used, can be a tremendous benefit to all, but that again we have got to have some processes that protect people. And the more we have seen of examples of abuse of the Internet that have hurt people, the more everybody comes to realize that industry must do so much, as has been indicated, to address the issues.

I think there are still some that -- perhaps it's a little like the wild West in the development of America -- who say, "Let not government be involved." But there was also the marshals and Wyatt Earp and others who brought some order to it.

And I think what we're faced with here is the -- something that I suppose humankind has dealt with throughout the history of the world. You don't like people telling you what to do, Pete. And there are going to be times when somebody tells you what to do, and you take issue with it and contest it. And then there are going to be other times you say, "Well, they were right." But there is just an instinct in us all to be free, and yet a recognition on the part of all responsible people that we have got to be accountable to each other.

What we're doing on the issues of law enforcement and what this report indicates -- this is a wonderful new medium, and we're going to have to take the lessons we have learned from all of time on how we balance freedom with accountability and apply it here.

Q Can we look at the opposite side of the coin? Secretary Daley, in your remarks in particular -- the Internet has a great deal of energy, a great deal of creativity. It's one of the engines driving the current economic boom. The tenor of your remarks seemed to be that we have to do certain things, but above all, let's not do -- or let's do no harm.

Let's not do anything to blunt the vitality of this new medium.

SEC. DALEY: I would say that's accurate, but that doesn't mean you don't do anything. And in answer to your question, the previous question, I think, you know, a mere seven years ago, there were only five websites in existence. This whole medium has just exploded in an incredible, short period. And we are, as government, and we believed, and as I said, President Clinton and Vice President Gore's policy of 1997 in that the private sector should lead, and the times they've only led by virtue of the fact that they've been kicked a little by government or the fear that if they didn't do something on privacy -- and three years ago there were very, very few if any privacy policies being put on the website; today, while over 80 percent, I believe, of the websites have a privacy policy that is clear and put forward in a fairly visible way for the users of the sites -- that's progress.

But I think it is, as the general has stated, it is a balance and it is trying at the beginning, when I think if creative people saw the enormous potential, they were maybe overly concerned about any sort of regulation and any government involvement, as they should have been, because it was very much in an infancy stage. I don't think anyone would say that we are still in an infancy stage of the growth of information technologies. What we are coming to grips with as government is that this is going to be probably continuing this enormous rapid pace of progress that makes it difficult for us to respond.

But we have to, as the general also stated, this report and the conclusion of the report is that we have to work with the private sector closely to identify ways that we can solve some of these problems for the good of the general public and for the good of e-commerce, so that people's confidence and faith as we all -- a few years ago, you know, it was really up to you whether or not you wanted to play in the game of the Internet and these new technologies. Today, you don't have a choice.

You're in there.

Q Ms. Reno, to what extent are these turf fights hampering your efforts to police the Internet? There are some reports about the Treasury Department, Transportation, and the Secret Service not participating in NIPC in ways that they -- in the full way that they could be. What's your feeling about that?

ATTY GEN. RENO: I think we are working well together. I think we are trying to develop the capacity and understanding of how we work together. If you had -- Commerce and Justice have had tensions over time. But as we work through the issues, as we understand better, as we see each other's roles, I don't foresee that these should be roadblocks at all.

Q Why aren't the agencies participating with NIPC?

ATTY GEN. RENO: Probably because of funding issues. And they are prioritizing things and feel like, with what have going, they can be a phone call away or an e-mail away. At any rate, these are issues that we have to build on. And as we develop and identify needs, we need to take action.

Q Ms. Reno, with regard to "people's desire to be free" that you referred to, do you disagree with the statement that individuals should be allowed to communicate anonymously using the Internet, so long as they are not committing criminal activity?

ATTY GEN. RENO: I don't do "what ifs" because I don't know what "so long as they are not committing criminal activity" means and I'd like to take it on a specific basis.

But I just think, again, the basis of this report is, "Let's sit down and talk about it and try to come up with answers."

That's what we did on the issue of encryption. And we had an excellent meeting with industry. They gave us new information. We agreed to be a better partner. And I think we can do it here.

Q Ms. Reno, something that civil libertarian critics have said, that there is no real evidence and widespread criminality on the Net,

particularly in this report. So why address this now? Is this just looking towards the future? Or is this in reaction to specific criminality and growing criminality on the Internet?

ATTY GEN. RENO: I think we have seen sufficient criminality on the Internet to be prudent and take appropriate precautions. And rather than do it in haste, rather than do it in a way that could adversely shape this wonderful medium for the future, let's do it in a sensible orderly way now.

Q Ms. Reno, regardless of turf fights -- in its sort of multijurisdictional context, does that mean there is going to be a growing role for federal agencies, regardless of whether the Treasury, FBI, Commerce, whoever?

ATTY GEN. RENO: What we want to do is to work with state and local officials and recognize that, as I have said, the physical laws should apply on the Internet. So under our principles of federalism should the state and local authorities be on the front line and have prime responsibility for the enforcement of laws within their jurisdiction.

Obviously, state boundaries are going to be as meaningless as international boundaries. And it is going to be important for us to develop new procedures with respect to exchange of information, securing witnesses' testimony and the like. But I am dedicated to doing everything I can to ensure that, along with privacy issues and other critically important issues, the principles of federalism are addressed, too.

STAFF: One more question.

Q How deep is the mistrust, on the electronic world's part, of government? How deep is it here? And to what extent has that mistrust diminished?

ATTY GEN. RENO: You want to answer that, Mr. Ryan?

MR. RYAN: Could you repeat the beginning? How deep is the mistrust?

Q How deep has the mistrust on the part of the electronic world been of government? And to what extent may it have diminished?

MR. RYAN: Well, I can only say at present times I think that's a false premise. I think --

Q (Off mike.)

MR. RYAN: Well, my experience is limited to five years, but that's half the life of this new medium. So I think I can still speak with experience. I think that, again, it's a false premise, that responsible industry leaders have worked and are committed to working with the public sector. There is a recognition that public safety is not an area where there should or is tension. It's in the mutual interest of both industry and the public sector to promote a safe and secure environment for everyone who uses this medium. The growth of this medium depends on consumer trust and confidence. If we cannot -- industry cannot provide a secure environment, we cannot expect members to engage in their everyday activities, which they have embraced today. So I don't believe that's a true premise, and that's not the way we interact now with the public sector.

Q So there's been total trust from the beginning?

ATTY GEN. RENO: I would sense that on the part of some industry representatives there has been concern and -- concern that law enforcement might try to regulate more than just prevent. And I think the more we can build a partnership and recognize that with cybertechnology has come an interconnection that makes it imperative that law enforcement and the industry and the industries served by the technology -- that we work together as partners. And I think with that theme, the distrust that might have existed is beginning to vanish.

Q Thank you.

SEC. DALEY: I would just say, if I could, one comment on that. In the three years I've noticed a tremendous movement.

The suspicion, skepticism three years ago on private sector -- about any of our activities, whether it was in the encryption area, in any -- even in a difficulty in getting them to engage with law enforcement, quite frankly -- that's changed remarkably over the last year or so.

It's -- the responsible, as Mr. Ryan said, companies understand that their future is at stake, and we understand that this is not just a passing technology, and that the benefits are enormous and widespread. So we've, I think, all changed.

ATTY. GEN. RENO: Thank you.

Q Thank you, and please come back. (Laughter.)

END.