Panel Two:

Information Policy Making

Panelists: Allen S. Hammond, Associate Professor and Director, Communications Media Center, New York Law School.

Bruce W. McConnell, Chief of Information Policy and Technology, Office of Information and Regulatory Affairs, Office of Management and Budget; Chair, Government Information Working Group, Information Infrastructure Task Force.

Michael Nelson, Special Assistant for Information Technology, Office of Science and Technology, The White House.

Janice Obuchowski, Annenberg Senior Fellow; President, Freedom Technologies, Inc.; former

Assistant Secretary of Commerce and Administrator, National Telecommunications and Information

Adminstration.

Marc Rotenberg, Director, Electronic Privacy Information Center.

Moderator:Fred H. Cate, Annenberg Senior Fellow and

Convener; Associate Professor of Law and Faculty Advisor to the *Federal Communications Law Journal*, Indiana University School of Law-Bloomington.

Mr. Cate: The afternoon panel is where we turn to consider the role of the government with regard to information policy making and law making. Is the complexity of issues and policymakers, in a number of different institutions, congressional committees, and courts, inherent in this area? Does it have an impact on the process? If so, is that impact something about which we should be concerned? Is there a need for new agencies, new congressional committees? Is there a need for centralization in existing agencies or committees? Is the Task Force process a way of working to combine and connect interested agencies without fundamentally changing the structure of government information policy making? Finally, as I

signalled this morning, we will be looking specifically at what role there is for regulatory forbearance—for addressing issues without necessarily regulating them.

Let's begin with the same sort of open-ended question that started the morning panel. What consideration is going on in the information policy-making process about the nature and role of that process itself? Are new policy-making structures needed? Is regulatory forbearance an issue of concern?

Mr. Nelson: Well, there is a lot happening. I work at the Office of Science and Technology Policy (OSTP). I report directly to Jack Gibbons, who is the President's Science Advisor, but I have also worked for seven years with the Vice-President on these issues.

It is fair to say that information policy issues have always been front and center on his agenda. It has always been one of the largest concerns, quite frankly, as we develop the information highway. When you look at all of the opinion polls you find time and again that people are excited about the information highway. They like the idea of having access to all this information, but they are very concerned about privacy and security, and to some extent intellectual property on the information highway.

At OSTP, I am actually involved in all pieces of the Global Information Initiative (GII) and National Information Infrastructure (NII) initiatives. We have a lot of things underway. We are trying to educate the public on the GII and NII initatives to share the vision. The Vice-President is doing that very well. We coordinate research and development activities. We are also promoting the use of this technology in a hundred different ways, and we are working with the Hill on telecommunications policy reform.

It is fair to say that information policy issues are the hardest issues, and in many ways are the least mature issues of all the things I work on. That is why I spend more time on this area than on the other four areas mentioned earlier in Panel One. I have had the pleasure or dubious distinction of being involved with the Clipper Chip debate.(1) I chair an interagency group on encryption and telecommunications along with a colleague from the National Security Council. That one issue shows how important these issues are, and it shows how they have the potential to get you on the front page of *The New York Times*, not once, but many times. And yet the Clipper Chip is just one small piece of a broader issue, that of encryption.

The Clipper Chip only relates to telephone conversations; it only relates to one specific technology. And, of course, encryption is just one small piece of the overall privacy debate in security discussions that we are having today. So there is a lot of potential for debate here. There are lots of different people with lots of different opinions.

In the area of privacy, you have the privacy advocates, who believe the right of privacy is the only thing that matters, the law enforcement community, that is very worried about losing access to wiretaps, and we have the marketing community that feels the more they know about their potential customers, the better.

In the area of intellectual property, we have similar balances to be struck. We have the radical librarians who say information should be free to everybody all the time. On the other end of the spectrum, you have the people who say, "It is my data, and I will sell it, and that is the only way it will ever be available," and they really do not see the need for libraries. In-between, there has to be an answer.

Security is the same thing. We have a balance between those who have brand-new technologies that they want to get into the marketplace and the people who worry about security almost excessively, who see any new technology as a threat to our national security and the security of data. So somehow we have to do all this balancing. That means you have to bring all the players to the table. And this is what we have attempted to do.

I used to work on the Hill, so I know how decentralized the policy-making process is up there. You have a number of different players involved. Until we came into office, I think it is fair to say that these issues were dealt with in a very decentralized way in the Administration as well.

We have made some order out of chaos through the Information Infrastructure Task Force (IITF), which was created by the President and Vice-President through my office and the National Economic Council. It is chaired by Ron Brown, the head of the Commerce Department. Under this Task Force, we have brought together all the key players for every issue that pertains to the NII. We have set up a privacy working group, an intellectual property working group, and a forum on security issues. We still do not have as much order as I would like. We still have a lot of different agencies that are not quite sure what their role is. Luckily, they are all around the table.

The privacy working group is headed by the Department of Commerce now, and they are bringing together each of the different agencies that has a role to play on defining privacy, and, as Bruce McConnell can expand upon, they have put out draft privacy principles.(2) Our intellectual property working group is headed by Bruce Lehman from the Patent and Trademark Office (PTO), but the important thing is that PTO has brought in all the other agencies that deal with intellectual property issues, from United States Trade Representative (USTR) to the various education agencies. We really are trying to bring people around the table, and in the end, we hope to have a very clear agenda with very clear responsibilities for each agency. These are the showstopper issues we are talking about. These issues could bring the whole discussion to a stop, if we do not deal with them properly.

I have this recurring nightmare, particularly in the area of security, where I think it is fair to say we have eight or ten different groups working on different parts of the security problem, that it is October 1996. Once again, we are saying the information highways are vital to America's progress and happiness. Then, some hacker brings down the air traffic

control system, Wall Street, and two-thirds of the nation's telephone system, and we are sitting there saying, "Oops!" We really need a way to ensure that we have an answer when that happens.

I will not talk about the international issues. I could go on at length. When I really want to get depressed, I think about the question of how we are going to deal with these questions in an international environment. Intellectual property and privacy, in particular, are areas where we have conflicting structures. Slowly, we are getting some international discussions. Last weekend, at the G-7 meeting in Brussels, these issues were on the table. Almost every delegation from all seven nations said we have to deal with these.

There were some very general questions to the World Intellectual Property Organization and to the Organisation for Economic Co-operation and Development (OECD) like, "Gee, these are some really big problems. Why don't you do some more work on them?" It was not specific, but it will be helpful in pushing them forward and getting more agreement on how to deal with privacy and security concerns—whether security of the Internet, or databases, or phone systems.

But, we have a long way to go. I fear that we are probably two or three years further behind in these areas than we are on the telecommunications policy issues. We are much further behind than we are on some of the technology policy issues I work on. Luckily, we have Bruce McConnell, Sally Katzen,(3) Bruce Lehman, and some other key people in the government working on them, and the private sector is getting increasingly involved in this as well. That is a very long-winded answer to a very good question.

Mr. Cate: Given that a number of the NII's working groups and sub-working groups seem to be addressing specific problems or areas of problems—for example, privacy and intellectual property—is there a place for addressing the metaissues: the freedom of expression issues and the framework issues?

Mr. Nelson: Well, those actually come together either at the committee level or even at the full IITF level. And often the Vice-President is the one who has to sort of broker a deal. I think the structure works quite well. The IITF has been very effective. In most of these areas, in previous administrations, we either had no policy or we had five policies, depending on which agency you asked. I think we have been able to do a better job of having one policy. The secret weapon, of course, is the Vice-President, who can "ride herd" on the agencies and can get everybody to march towards the common vision.

I will not say that we have moved as quickly towards that vision as I would like, but I do think we have the right people in the room, and we have a way now to resolve these issues. Encryption is a good example, because we have an issue that pertains to national security, to competitiveness, to law enforcement, to international relations, to research —the whole gamut—and we have a team that is actually pulling in all those issues.

Mr. Cate: Is there talk about the continuing role of agencies? For example, you spoke about the Task Force serving a role of helping to identify a set of marching orders for each agency. Is there consideration of combining or altering the roles of agencies?

Mr. Nelson: In the area of privacy, in particular, we are certainly looking at a more formal structure. This was something that came out of both the IITF and the Vice-President's reinventing government effort. There is an understanding that privacy is so fundamental to the success of the NII and to the success of some of our reinventing efforts, we could benefit from a more structured approach.

We are evaluating the idea of some kind of privacy board, somebody that would not only lay out principles for privacy protection, but would also work with agencies to see that they are properly developed, and perhaps even more important, work with the private sector to see that those principles transfer into commercial applications as well. In the last twenty years, people have gone from being really paranoid about government and Big Brother to being really paranoid about government—Big Brother, American Express, Safeway, and whoever else is collecting data about them.

Mr. Cate: Janice, how do you see this sort of policy making—the information policy-making business of government—changing or developing?

Ms. Obuchowski: Well, that is a good opener. This interest in these issues tends to have had an ebb and flow, even over the last fifteen years. When I first came into government, I remember going over to the National Telecommunications and Information Administration (NTIA), and at that point in the early '80s and late '70s, the "IA" really stood for a very heavy involvement in information issues. I think as the decade moved on, interest in information policy almost was given a back seat over the dynamic developments in the sort of "divesture era," the introduction of telecomm competition. I think it is really good news that this Administration is putting the "I" back into NTIA and is just putting the information policy issues back on the front burner.

A question of the role of government is always very difficult to address in the information area. It is difficult to address, because government has an easier role where answers can ultimately be worked out. If you are running a program or enforcing a law, you can set up an agency, or you can put in a prosecutor. But as Anne Branscomb so eloquently points out in her book, when you look at this whole area, there is an inherent dynamic tension between property rights and privacy rights.(4)

If anything, that is the bottom line in this debate. There will always be a dynamic tension. There is no way around it when you are talking about information. There will be people who claim the right to own it, and there will be people who claim the right to privacy. You also have other issues like control and trade implications that flow out of that inherent dynamic tension. So you tend to wind up in a circumstance where you do not have a single right answer, but you have principles or trade-offs that you are making, and it is always very hard for government to enforce trade-offs.

So with that sort of context, I think in the information area, the Clinton Administration has been farsighted in raising this debate. I believe they have the right people around the table. I tend to think they are doing what is smart, without getting into the details in some cases where I might disagree on how the principles shake out. You cannot, in the end, legislate here. You have to come up with some core, bedrock principles that balance this dynamic tension. And the process is as it should be. I would not be overly pessimistic about the fact that government is not ahead of this game. I do not think in the field of information, the government is ever going to be ahead of the game. How can it be? This is a just-in-time issue, as people point out. Property rights are very difficult when it comes to information policy.

As Diana Daniels, in the audience, will tell you, *The Washington Post* is not worth anything the next day. So it is a different kind of property right than almost any other kind of information. It is a just-in-time issue, and I think government, almost by definition, cannot move that fast.

I would like to raise an ancillary issue here, which is not directly on the table. Whenever you are working in this area of information policy, I think you can't ever be too far away from the sort of telecomm policy issue of open platforms, because one of the ways to resolve this dynamic tension of who controls information, who possesses it, becomes the issue of ways to ensure that people in society all have good sound and multiple sources of access to the information.

Mr. Cate: Bruce, tell us more about what is happening, and are we, in fact, going to see this Administration process get ahead of the curve, or is Janice right, are we always going to be playing catch-up in the information world?

Mr. McConnell: The short answer is, the Administration is on the curve. Some agencies are on the leading edge, and other agencies are on the trailing edge, but they are all on the cutting edge.

It is fun to be here, on the cutting edge, particularly to talk about the nontelecomm parts of the Administration's work in the NII, because this is a place where telecomm is often talked about.

There is a difference in the way federal and state governments need to attack this question, as opposed to the telecomm questions that are often discussed here. We are much more constrained and limited in our role than we are in what is traditionally a regulatory approach on the telecomm side.

Not only are we not going to *build* the information highway, but, in fact, in this area our best role is as a facilitator and catalyst to make the discussion happen among the people in the private sector who need to really implement the solutions. There is some policy work and some framework that we can lay down, and that is what we have been trying to do in the work that Mike was describing. The fundamental premise that we are operating from is that if people

cannot trust the information highway to send their information when and where they want it to go and under the terms and conditions that they want it to go—and only in those ways—then they are not going to use it. They won't realize its potential and the valuable information will not flow.

On the specifics, we put out a paper in July, 1994—a green paper— that deals with the intellectual property implications on the NII.(5) The report focused primarily on copyright law, and its conclusion was that it still looks pretty good although it may need some minor tinkering.

There was some discussion in the paper regarding the need for technology to prevent copying. The reaction we got—and we got over one hundred comments and reply comments—was that we seriously underestimated the complexity of the problem. There was agreement on the report's emphasis on educating people about the importance of copyright, particularly in the area of software and digital works. But, the technological issues are much more complex, and the technological solutions need more discussion. Also, the questions of balancing of owners' and creators' rights with the needs of users, and the whole issue of fair use need greater exploration.

One of the most important places we are getting comments from is the National Information Infrastructure Advisory Council, which is an advisory committee that is advising the Administration on all of these issues. It has provided some detailed comments on the report, which are proving very helpful to us, in terms of rewriting it. And on the fair use question, there have been some conferences that the PTO has sponsored to start discussions in that area.

So, we have a lot more work to do there than we thought. We hope to come out with another version of the paper in the spring.(6) It is not clear at this point how well we will treat some of these issues, but I think we have learned that there is more to this.

On the privacy front, I guess I share the view that the government is not the only problem at the moment. Privacy, of course, is not an absolute thing. With absolute privacy, you wouldn't even be able to do business. So the question is: How do you come up with a balance?

We put out these privacy principles last year, in May, and we have put them out again for comment,(7) and they are also being discussed by the NII Advisory Council, who has put out its own set of principles.(8) If you look at the various principles that are around, they are pretty straightforward. You should be able to give consent how information about you is used. You should be able to go look at the information and correct it, and you should have some right of redress if you are harmed by uses of it that are not authorized by you.

How you strike those balances is going to be different in different circumstances and for different sectors. You are going to treat health information slightly differently than driver's license information. So the principles are designed to be general guidelines, and it may be necessary, in some cases, to do legislation. At the moment, there is no comprehensive federal privacy statute. It is illegal to disseminate someone's video rental records, but not their health records, at the federal level.(9)

On the question of whether there should be a federal organization that looks at privacy, either an independent regulatory commission, an independent nonregulatory commission, a board of some sort, or something inside the executive branch, as Mike said, we are looking at that. Again, there is a double-edged sword. Do you really want the federal government looking at the privacy issue, and having the ombudsman function? But on the other hand, at the moment, there is no central focus, except to the extent that we at OMB spend a little bit of time on that. There is also an international aspect—other countries do have privacy boards.(10) There is some question about whether that would be useful for us to have one as a trade-balancing device.

A third area, computer security, is a very fascinating topic. It is true that the Clipper debate has increased attention to this issue, but it also has had negative effects. One of the negative effects is that it focused the question of computer security on the question of confidentiality, and, in fact, computer security means a lot more than that. It means making sure that information's integrity is retained and making sure the system is there when you need it.

What we have been doing to try to tackle this larger question has been to conduct a series of public meetings. We have had five public meetings so far, and we are going to have another one in March, on the question of security in the

National Information Infrastructure.(11) These meetings have been focused on specific sectors, for example, what is needed to protect intellectual property, and we bring in intellectual property producers and users and try to learn from what they think their requirements are going to be. We hope to put out in the spring a report that suggests what we have learned from these meetings. We are calling it, rather ambitiously, an NII security plan.(12) That is only there to get your attention because, in fact, we are not going to be planning this at the federal level. This is something that is going to have to happen mostly in the private sector, but we are trying to use our catalytic role here to put this out for comment and get some discussion going.

The final area I will mention briefly. We are trying to use the information highway ourselves, as a government, to make government information available. We have a great number of home pages up on the Internet, and we've got a lower-level service, Fed World, operated by the Commerce Department, which has over 100,000 registered users, so we are getting quite a bit of government information out electronically.

We also have started a program called the Government Information Locator Service, which is basically an electronic card catalog. By the end of the year, agencies are supposed to have figured out what information it is they have, which they do not all know, and then begin to put a listing of those holdings up on the Net, so that people can look for them, and ask for them, and get a hold of them.

This is all being done under the general auspices of the IITF. I was asked yesterday by some folks in Quebec who have not used many working groups how well these working groups work, in terms of getting stuff done. My response was that they work best if there are a couple things. One, there is accountability in the members to be responsible for things, so that you can embarrass each other in the working group—why haven't you done your work? But the other thing is, they work better when the working group has a specific set of defined tasks.

In the policy-making area, that is hard. There is no specific defined task, it is, rather, "think about this and come up with something," so it is very slow as a policy-making mechanism. But if you do get the right people together, then you can get some to buy into the policy as it is developed. So it is a mixed bag, as far as that goes. Of course, working groups have no authority to issue any policies, so then you have to find somebody who has stationery to write the policy down on and send it out, but that is a smaller issue.

Mr. Cate: Allen, what are your perspectives on the extent to which the diversity of issues are being dealt with by the diversity of agencies that seem to be involved in this process?

Mr. Hammond: Well, you couldn't create a list of all the possible issues. I tried just briefly, and I came up with twenty-one. I must have left out over one thousand. If you look at the number of agencies and governmental bodies that are involved, and they range not only from the committees that the White House has wisely set up, and the Congress, and agencies like the Department of Justice and the FCC, but the courts, the states, and, of course, cities as well, many groups are concerned about these issues.

So if you had to go to a forum to resolve these issues, where would you go? Technically, you would have to go to all of these different forums. That creates some very great difficulties. Historically, one of the problems with developing policy in these areas has been that you run the risk of it being ineffective, because it is so fractured. To be fair, the government's response, in terms of interagency and interindustry committees, is not accidental. I think it is very wise.

But I do have a question, once you come up with a policy or policy recommendations, where do you go? Do you go to Congress? Do you go to the courts? Do you go to the FCC? Do you go to the states? Do you go to all these places? And if you do have to go to all these places, aren't you back into the same problem or difficulty with checks and balances that we have experienced, for instance, with regard to S. 1822,(13) and H.R. 3636,(14) and now the Pressler proposal?(15)

I am not so sure, however, that that is all bad. It is a deliberative process. It should be democratic. It should have all the parties involved. We should have to debate this thoroughly, because it affects us all.

I am curious, though, to what extent these committees can perhaps create a de facto standard in some of these areas, and create a de facto standard, in part, because the government is such a big producer and user of information, perhaps

in much the same way that some argue that the Clipper Chip might have become a de facto standard in encryption. Since so much of what we have been doing is involved with the government and the government has control of it, then, the government by making decisions about how it uses its information, how it provides information may, in fact, make a number of determinations about how the rest of us may use information as well.

I guess I am sort of old-fashioned in the sense of being a lawyer in Washington for so long. I got used to the idea that there are a lot of different agencies to whom you had to go, and that you expected a process to develop—from a policy at the White House level to proposals, perhaps, to the FCC, or deliberations in Congress, to actual legislation, to litigation on the legislation, to some resolution, and, again this is showing my bias, by the Supreme Court. But this will not work in this case, I do not think. Certainly, efforts on the part of the White House could create some sort of consensus. It is probably wiser. It sort of appears to me to reflect more of a European notion that we cannot always rule by fiat.

Mr. Cate: Marc, you have been both a participant in and a critic of the policy-making process, particularly related to data security and privacy, as well as other issues. Not limiting yourself to that, though, how is this process going, what should it be doing better, or what is it doing perfectly well?

Mr. Rotenberg: I think there is an aspect of this process that has a very strong sense of unreality about it, a theoretical detachment from practical problems and real issues that is producing policies, but do not translate very well into the real world.

Mike and Bruce mentioned the privacy working group and the effort to move forward on the Clipper Chip proposal. It would be hard to find a less popular information highway-related proposal to come out of Washington in the last fifteen years than Clipper. And if that is the case that you make for a government working group, I think you have to do a little rethinking. But to be a little bit more precise, to put a fine edge on this argument, I would like to read just a few paragraphs from the front page of the business section. This is yesterday's *Philadelphia Inquirer*. The title of the lead story is "Bell Failed to Protect 13,000 Callers' Privacy."(16)

The customers had signed up to block their phone numbers from Caller I.D. Despite that, their numbers were revealed. When Bell Atlantic Pennsylvania began offering Caller I.D., it promised to protect the privacy of those who didn't want their numbers disclosed, "[b]ut yesterday the company revealed that it accidently failed to protect 13,000 of the 112,000 Pennsylvania customers who believed that their numbers would not be displayed to anyone with Caller I.D."(17)

Now, I could go off on a little privacy rant and tell you about the evils of Caller I.D., and how we could have told you this was going to happen. But I am not going to do that today with this group, first of all, because you have probably heard it, and secondly, because the role of government in the story is even more interesting.

What is the role of government in the development of the information highway? Let me continue. The story picks up. "In June, the State Public Utility Commission authorized Bell to offer the service. Yesterday, PUC officials said they were dismayed that they did not know the problem existed until Bell announced it had been fixed. They questioned,"—see, now you are catching on—"They questioned how long Bell had been exploring the problem, and said the company's error could amount to a violation of state law."(18)

"`What did Bell know and when did they know it?' asked Tom Seaman, the PUC's legislative liaison. `It is a little troubling that Bell takes it upon itself to correct and announce the problem and ignore the PUC.'"(19)

Now, even for people who may not be so sympathetic to the concerns about privacy and Caller I.D., I hope you pick up in this story that there is a serious problem emerging in sorting out what the appropriate role of government is in the information highway. I think this problem is most acute in the privacy realm, and I think this, in part, because currently the U.S. is of the opinion that through voluntary guidelines, self-regulation, and industry practice, we will be able to address the privacy concerns of American consumers.

In fact, this was the position that was brought to the G-7 last weekend in Brussels by the United States, echoing the OECD comments of 1980, the principles which underlay the 1974 Privacy Act(20) contained in the 1973 Health,

Education, and Welfare Department report,(21) that a code of fair information practices will be adequate.

Now, I would say that is sort of hands-off driving on the information superhighway. That is kind of getting behind the wheel, pressing down on the accelerator, and not being too concerned where you end up. And, frankly, for policy making, whether it is in privacy or in other realms, it is not going to take you where you want to go. It will take you somewhere, without question, but there is a very high probability that you will end up on the side of the road.

I would just like to add two points to this. I had an experience, one of those conversion experiences. Everyone has a conversion experience at some point in their life. I had my conversion experience in 1990, when I first heard about the proposed offering of the Lotus marketplace product. This was a series of CD-ROMs, based on data in credit reports that was enhanced—to use the direct marketer's terms—enhanced by public information, and to be sold to American businesses.(22) I did some research on the product, and I noticed that the Direct Marketing Association had a code of information practices. One of the principles contained within the code said that customers should have an effective mechanism to opt out. They are trying to avoid a government regulation. They want self-regulation. They think this is an appropriate approach. And by the way, this is still, today, the standard for protecting consumer privacy. You have an opportunity, through the mail preference service, to opt out of the sale of marketing lists.

I talked to the council for the Direct Marketing Association before the product was released, and I said, "Well, I think you are going to have a problem here, because what you are talking about is essentially the equivalent of publishing unlisted phone numbers, unlisted addresses, information that people have not consented to be publicly disclosed, and then saying to them after the fact, `If you object to that, contact us and we will take your name off the next edition.'"

I said, "I don't think that is a very effective opt-out." It seemed to me that if you are going to enforce your code for information practices, you would be obligated to ensure that that product is not released, at least not released as was currently designed.

They said, "Well, this is a very interesting issue, and it is something that we will have to look at closely, study, and discuss among our members and see what is appropriate for us to do."

But, of course, they did nothing, absolutely nothing. The Direct Marketing Association did not object to the release of the product. And it took, in fact, 30,000 people sending electronic mail to Jim Mansey(23) at Lotus to see that the product was not released.

Now, there was a lesson here. There was a lesson about the adequacy of fair information practices, and what happens in a policy environment where government takes this hands-off approach to consumer concerns about these types of issues. Obviously, I am focusing on privacy issues, but I suspect there are other areas that you would be familiar with where this analysis would apply.

I am going to make my final point here about this argument, and that is, I think these problems are going to increase. I do not think we have had the last Lotus marketplace incident. I do not think the *Philadelphia Enquirer* is the last paper that is going to write about privacy concerns with new communications services. I think you are seeing the beginning of what will soon become a flood—a flood of public concern and public protest about the inadequate privacy safeguards in many of these new service offerings. And then the issue is going to be forced upon government and upon people who would choose to serve in government to respond to that old-fashioned political need: how to protect the public interest. And at that point, these issues will become very real, and the unreality that does characterize, for the most part, what has been produced to date, I think by necessity, will recede.

Mr. Cate: I take it you are not satisfied with the draft privacy guidelines coming out of the IITF?

Mr. Rotenberg: I think that is a fair conclusion.

Mr. Cate: Is the reason for that a failure in the process? Has the public anxiety you are talking about not yet been heard from? Was it heard from and ignored, or is it the type of process that would not receive that comment? What can we say about the process that led to the result that you are not happy with?

Mr. Rotenberg: Well, I think on that multiple choice I am somewhere between "B" and "C," which is to say that there was, first of all, a translation process, because the level of public concern has been established. It has not yet been translated into enforceable law, and into enforceable right, so that is a translation process.

But there is also a procedural process. There is a procedural process, for example, when you create an intra-agency working group on privacy among all these agencies where there are various mandates, except there is no agency with a mandate to protect privacy. So you have this very peculiar situation, where all these people, in effect, say, "Well, if I were responsible for protecting privacy, I imagine that my agency would take this position." And you can have ten of those people, or you can have thirty of those people, but in the end, you will get no closer to developing a privacy policy. This is the story about the emperor's nose. If you have not measured the emperor's nose, it does not matter whether you ask one person or 1000 people how long it is.

Ms. Obuchowski: Aren't there sort of two separate issues here? The one issue is the public concern about privacy. And the public's concern about privacy, from my observation, is that 99 percent of the time the public seems almost indifferent to its own privacy. People don't think about where they send their credit card information. They don't think about what happens to their checks. They enjoy getting junk mail, until there is an incident. And the 1 percent of the time that the public just goes off the charts out of concern is where something absolutely outrageous happens; it is picked up on a talk show and someone says, "My gosh, that could happen to me." And then, in sort of an incidental or episodic fashion, the public gets really concerned.

I happen to be one of those folks that, 99 percent of the time, doesn't think too much about my privacy, and when I get serious about it, and consider what people might know about my life, you can never rule out a despot, I say, "My gosh, we've got a looming atomic problem here." So I don't think it's quite so easy to characterize where the public is on the Richter scale.

But there is a second issue that gets to the role of government. The public has a great distrust of the government as a guardian of privacy, and probably rightfully so. I'll use a case out of the Clinton Administration. Members went into the State Department's files of some people that were in the last Administration and used it for political ends, and that happens time and time again.(24)

So the fact that the public is concerned, I am not sure leads to any given conclusion as to government action. Because if there is one thing that concerns the public more than their privacy, it is government invading their privacy. That is when you get into this funny kind of thing where people—a lot of Libertarians and ultraliberals—will have the same views on their own privacy and then have very different views on the solution.

Mr. Rotenberg: I think you made a very good point, but let me suggest to you that there is, nonetheless, a problem in sort of framing the question in the sense of, "Can government do anything in this area that doesn't cause further damage?" It is a very common criticism of proposals, such as the creation of a federal privacy commission. People will say in the first sentence, "We don't want government protecting our privacy."

I found it quite extraordinary over the last couple of years, as I have looked more closely at privacy regimes, both in the U.S. and abroad, to consider the fact that the U.S., which, as I said, has taken sort of this general hands-off approach to privacy protection, has marched down the road toward a technical scheme developed by one of its intelligence agencies to permit network monitoring called Clipper. On the other hand, the European countries that are still struggling somewhat with a debt-protection directive, intended to harmonize their safeguards, have moved toward a technical scheme that is much more privacy protective. What I draw from that sort of, as I say, "flying over 25,000 feet," is that if you make a commitment and you say, "Well, privacy is important, and we are going to try to do something to protect our citizens and our consumers," and so forth, I think you are more often likely to get it right than you are to get it wrong.

In looking at the technical outcome and comparing the U.S. to Europe, my sense is that the Europeans are more likely right now to get it right than to get it wrong, because they have made this commitment. This is important, too, because you see, with some of the people who would say in the U.S., "Well, we don't want the government to be regulating all this stuff; We don't want those European-style commissions," it is the U.S. Clipper standard which has the most concerns. So there has to be some careful assessment of who is making the commitment to safeguard the public

interest.

Mr. Hammond: I think what both of you said is right. I think there have been some standards that have been developed. Again, being a lawyer, I am going to point to the courts. There have been instances in which the courts, if not the Congress or the President, have fought to protect privacy interests and privacy rights, and have sought to protect, or at least penalize corporations for the downside risk or the downside damage that occurs when information is misused. I would assume, and I would hope, that this has been incorporated into the policy directives that are being proposed.

But, quite frankly, it is my suspicion that regardless of what the White House does through its policy committees, the controversy is going to end up in the courts anyway. Sooner or later there are going to be instances in which people deem their rights to have been violated. The courts are going to take an equitable approach and a constitutional approach to the finding, whether or not, in fact, there is an expectation of privacy there, and whether they are going to penalize the corporation or the government for being involved in it.

Mr. McConnell: I have three comments on the discussion that has just occurred. One is that I agree with you, Allen, and with you, Marc, that principles are not enough, and, in fact, that legislation is needed. The reason for coming up with general principles is to start with a general framework. Our view—and maybe we are wrong—is that the legislation that you need in the health area may be different than the legislation you need in the banking area. It needs to happen on a sector-by-sector basis, at least to some extent, with respect to privacy. I couldn't agree more; litigation will follow, and work issues out. So this is the beginning of a process which, as Mike said, is behind.

The second point I would make is on the question of who constitutes these working groups in the government. This is a typical example, I think, of what happened when the Clinton Administration began. The Clinton Administration came into the White House with the idea that it is important to protect the public interest and the interests of consumers in a variety of areas, and that information is important, and we need to work on it. So it looked around and said, "Who can we get to work on that in the government?" since that is where they were, in the government.

In the case of privacy, we do have people in the government who have thought about privacy ever since 1974, when the Privacy Act(25) was created. We pulled together some people who think about privacy every day in a narrow way, really, in a way of, "How do you protect information that the government holds, and what are the procedures?" But these were people who had thought about the issue on a full-time basis for some time. We then brought in the public to contribute broader ideas. I agree with you, Marc, that by themselves, these are not the right people to do it; they were the only people, though, who were around to do it.

On the third point of the Europeans versus the U.S., I guess I would draw a different conclusion from the same facts, and that is, that we were just recently visited by some representatives from the French government who say, "This Clipper debate you've got going here, we're about to have that debate here in France. We want to know what you have done right and what you have done wrong, because when we go through this thing, we want to try and learn from it, because we are going to have the same problem to deal with."

In fact, the United States is the first place to have a public debate about this issue and about the balancing between some governmental interests, which are societal interests, in law enforcement and individual rights in privacy. At the end of this debate, we may have come up with the right answer different than from a command and control approach that is being taken in Europe. So I think that will be an interesting thing to watch.

George Papapavlou:(26) I am not an expert on security matters. I deal more with privacy, intellectual property, and other legal issues. But I think that probably on security issues, the fact that in Europe we are slightly behind in making decisions is largely because of all those inherent conflicts that there are and also because in different Member States there are different priorities. And it's true that probably the French are more strongly reluctant to allow security, encryption, etc. for private-sector use. It is probably also because of the condition of the public-sector role in France, compared to the U.K.

However, in the directive on privacy there are specific provisions for appropriate privacy-oriented security ends.(27) In Brussels, the commissions who work on the security try precisely to find ways in which, for example, anonymous use

of the new technologies can be made without damaging security or other issues.

I would like to make two more points. One is on the sectoral approach to legislation. I understand its historical origins and why it is so in the United States, but, of course, it may lead to the situation which Mr. McConnell mentioned, that you may have a law on video, but not on medical data. It is probably because there has been, I don't know the story with the video law, but probably there has been a scandal on a talk show. And that results in a law being taken to Congress by somebody who was affected by this scandal or something, whereas there has not yet been a scandal in medical data. It is probable that this may happen. With such ad hoc laws, there is no possibility to go to court or to protect your rights, because what has happened is legal until it is declared illegal, and if you have no general law, then many areas which you have not thought of remain outside and may create problems. If you have a general law, omnibus-type laws, as in Europe, you would probably avoid the situation in which there will be a problem, and there will be nothing to take care of it. At the moment, however, in the United States those who are against regulating the private sector have the upper hand.

May I finish with a statement on the possible board of control authority? In the morning and this afternoon, speakers have said that there is concern in the United States against giving such control to government. Does such a body have to be a government body? Couldn't it be a body which was formed—and I will use the French example—of senior judges, important personalities, and social personalities? The chairman in France is an ex-director of the most prestigious newspaper, *Le Monde*, and there are some councilors of state that are senior judges. And there are some other personalities. So there is a mixture of people with some expertise. There are some lawyers who would do the groundwork.

And could it be not accountable to the government, but accountable, for example, to the Congress? This is the German approach, where the Data Commissioner reports to the Parliament in the different states. Congress then would not be government, and the group itself does not have to be a government body. There could be options which would avoid this fear that the government is controlling privacy.

Ms. Obuchowski: Well, I think that the last suggestion is very worthy of consideration in the United States. I don't think that a government board is the answer, given the legitimate mistrust Americans have of government's own role in privacy.

Having said that, setting up a board which could, in fact, be reviewable by the courts, to my mind, would have a very salutory effect, if properly structured. It could help remind us of privacy issues about which we are, as a population, often indifferent. People like us—academics, bureaucrats, whatever—in our own world, somewhat disengaged from what is happening in the 7-Eleven in Dubuque, thinking these thoughts, and then sort of "disconnecting" with what might be happening on the street. So I think setting up a board or some kind of entity, which, in a disciplined way, addressed these issues, talked about these trade-offs, might have a very good effect in this country, just educating us generally as to what we possibly already have given up by way of privacy right, and how we might reclaim it—how we can make some of these trade-offs. My preference, if we were to do something like this and it had binding authority, would be to have the board answerable to the courts. The Administration and Congress both tend to have less public esteem in the United States as a detached entity than the courts do.

Mr. Rotenberg: Let me just say, Janice may be interested to know that the privacy advocates in Washington generally had quite a better success pleading their case with President Bush's Administration than we have had with President Clinton's.

Ms. Obuchowski: I am not surprised by that.

Mr. Rotenberg: Well, part of the answer you will be interested to know is that there was an entity that had this quasi-status, and it was called the U.S. Office of Consumer Affairs. It was headed by a Bush appointee named Bonnie Guiton Hill,(28) who sat on the President's domestic council, who was very much concerned about privacy issues, who testified on the Hill on many occasions on these issues.

I would say that that does not go far enough. I do not think education is necessary at this point. I think we have plenty of that in the papers, but I think we have to sort of open our eyes a little bit, and George's suggestion is a good one,

that it helps us move forward, where it seems in the past couple of years we have moved back.

Mr. Hammond: I also think that is a very good idea. In the first instance, it would be a nongovernmental body.

Mr. McConnell: Who pays the salaries?

Mr. Hammond: Well, that is something we will have to work out.

Mr. McConnell: It's just that I come from the Budget Office, you know.

Mr. Hammond: Well, I will give you an example. I chair the cable television committee in my city. We do not get paid, but we are, in essence, quasi officials. And we do have public hearings, and we do make decisions about the law and how it is going to be applied, and we do get a lot of flack from the citizens, because they don't like what we have done. So you don't necessarily always have to be paid to take some responsibility for being a citizen in this society. Maybe that is the quid pro quo for being a citizen, that you take some responsibility.

But the value of having some sort of commission, or some sort of an entity that listens to complaints, studies, and educates is that you then have one centralized location where the various types of circumstances that arise can come together. And then the courts, if they are to take an active role, have at least a coalescing of episodes, incidents, and circumstances with which they can then develop a more common law and common sense approach to developing some balance between the various rights and interests.

Richard Firestone:(29) As a premise for the question, I have some historical perspective. In the '70s, there was a privacy protection study commission—an electronic funds transfer task force that dealt with privacy in monetary transfers. There were interagency task forces under White House coordination and direction. There was legislation proposed, sector-specific, to deal with individual problems and not try and take a one-fits-all approach. There were surveys that showed this was a major issue for the public—a great deal of concern. There were documented cases of abuses or scandals that were put out in all the reports. Nothing passed. Nothing happened, as a practical matter, out of most of that effort.

Now the temptation is to say that we have new advisory commissions and interagency task forces, and we are talking about sector-specific legislation and the rest—and isn't the situation substantially the same? But let me take one other historical example. The cellular industry had an interesting problem, which was the public thought that cellular phones were secure, just like their home phones were, and they were not. They recognized at some point that the growth of their industry was dependent on changing the public perception and changing the legal implications and risks of using cellular phones. Digital technology and scrambling was sometime away, but suddenly the industry got behind a proposal to draft a law and enact it to restrict the scanners and things that would access, at least easily, cellular phones.

Suddenly, in a very short period of time, with relatively little public controversy, there was a privacy protection measure passed by the Congress, and signed by the President, and the law because it was viewed differently. It was viewed as necessary to move the industry and the technology forward.

So by way of not saying the '70s analogy is necessarily the one that fits today, Mike Nugent and a couple people this morning made a comment about how privacy security might be showstoppers for the growth of information technology. If the participants trying to build those markets and industries come to that realization, then there might be solutions that are passed, as opposed to just task forces, meetings, announcements of principles and things. I would be interested in the panelists' views of which is more likely to be the case now: Are we going to have lots of studies and nothing adopted, or perhaps industry-driven changes if and when we actually see solutions?

Mr. McConnell: I just have two comments, one on your premise. I guess I would say that the Privacy Act of 1974(30) was not anything. The other point concerns the power of sectoral protection. The public demanded action after the disclosure of video rental records from the Judge Bork hearings. So if we have enough of those incidents, maybe we will cover the waterfront.

I think that this approach is, in fact, probably more likely to produce results. What I find principles useful for is as a

benchmark to evaluate specific proposals against legislative proposals—whether they be privacy proposals or whether they be proposals to create databases for all illegal immigrants.

Mr. Cate: I want to follow up on this point by going back to the "unreality" problem. We are looking at a policy-making process that is most likely to be, at best, ineffectual and, at most, outdated by the time that it ends. While Congress and the FCC debate video dialtone, and cable-teleco issues, the federal courts are knocking each other over, recognizing the First Amendment rights of common carriers,(31) despite the fact that Congress does not.

Are we going to see the same phenomenon with privacy? Privacy, as Mike said this morning, is going to be one of the show-stopping issues. Yet, we are seeing twenty years of task force after task force after task force attempting to solve the problem, and still nobody seems overly happy. We have already identified that Marc does not seem to think there is adequate privacy protection. I assume that there are people who would be concerned on the other side of the issue as well; they don't want to see more regulation. They don't want to see government regulation. What is the level of optimism in this group that we are accomplishing anything here? Marc?

Mr. Rotenberg: Let me try and answer that question, also to the original question, because I actually think the original question was very important for our purposes. It is true that many of the privacy laws that came about in the '70s and '80s were the result of, first of all, some public education, some government study, and some industry self-interest. The Communications Privacy Act(32) is a very good example of that. The Privacy Protection Study Commission, which came about in 1977, was actually after passage of the Privacy Act, and it resulted in a compromise with the White House in lieu of the Privacy Commission.

They said, "Well, let's study these issues, and figure out what more needs to be done." I think there was a sense in the late '60s and early '70s that there was a problem and that we needed to address this problem to protect the public interest. You see this reflected in a lot of the early hearings, and the Health, Education, and Welfare (HEW) reports, and I think, frankly, more of an optimistic view about the role of government, and what government could accomplish. I think that has changed. I think, first of all, people are much more critical of government and its abilities today.

I think there are also those, particularly people in this room, who are much more skeptical about the likelihood of finding solutions in these rapidly changing technological environments, since the risks of guessing wrong are so high. Of course, it is on this side of the ledger that we understand the argument for deregulation and for not putting cement on top of the flower bed, as it were, as some of these new technologies are developing.

Now I will mention as a counterpoint to what I said a couple of moments ago. I came just before this meeting from, frankly, a long discussion I had with Senator Exon (D-Neb.) about his proposal. Quite a few people are concerned about the potential impact that Senator Exon's bill would have on the development of networks, because at the point that you begin to regulate content, indecent or luciferous, whatever it happens to be—suddenly you can have an enormous dampening effect on the flow of information. So, of course, our argument to Senator Exon is that you really have to be very careful in these new communication environments on how you regulate. A computer network and an Internet news group are not the same thing as a telephone. There are differences. And to borrow from one area to try to legislate, I am trying now to get to your point Fred, you can have repercussions that you don't want.

Now, obviously, that argument could be applied equally to some of the claims made on behalf of privacy. I mean they could say, "Well, you know, I agree with you about privacy, but if we regulate in this manner, this could have this unintended consequence, particularly in this rapidly changing technological environment, that we don't want to have." I think that is the debate that should be taking place right now in the United States on the privacy issue. Once there is commitment to protect the interests, then we sort through the problem of how to put in place appropriate policies. I don't think that the same could be said for Senator Exon's proposal.

Mr. Hammond: I go back to something I said earlier in response to the proposal that we have a commission. In response to the language that might evolve in this area, I think a common-law approach is the more logical approach, especially where we don't know how things are ultimately going to evolve. You allow the various considerations that arise on a case-by-case basis to become the basis for determining over time concerns that continually arise, and you develop some sort of a balance and structure in that manner. I am not saying you do it through the courts. I like the idea of a commission with review by the courts.

I think that would be a way to identify some fundamental principles, and arguably, there have been some that have been developed to date. For instance, those who have control of the information should take responsibil ity for any damage they do by virtue of mishandling the information or misusing the information. I don't think that is inappropriate. If we had such a commission with some flexibility to hear a vast array of different problems and cases, over time we would develop the kind of considerations that are necessary to put a policy and a law in place that we would be comfortable with.

Ms. Obuchowski: I would in general endorse that concept of a common-law approach. I don't know that this is exactly criticism of the Clinton Administration's approach. I think in this area of privacy—as in a lot of areas where the Administration has adopted the task force problem—what I see is the same of people, who are, almost in every case, very, very smart, trying to devise a cosmic solution to an almost cosmic problem. Having been in Washington long enough to be a realist, I think back to a guy—this is a digression into telecomm, I regret—but a guy at the FCC, some of you may remember him, who decided he was going to disaggregate the entire cost structure of the telephone network, and he was going to do it on a map on his office wall. And if you can imagine it—this is the truth—he was in there for ten years, and the map went around three walls, and he had only taken out one of seven features of the network.

That seems frequently to be the issue, as I observed the Clinton Administration on things like health care or telecomm policy. I would never quarrel with the intelligence level. I just think when you get into something this cosmic, and try to come up with a cosmic solution, you almost invariably run the risk that real life gets ahead of you. So somehow as we go forward, you do want people standing back and thinking big. So I don't want to close down these task forces. But then again, I think the advantage of sort of a bottom-up, a percolation approach, which is the common-law approach particularly if it is informed by a more educated citizenry—might yield some more concrete results.

Mr. McConnell: I would like to respond to that by being encouraged that you see the Clinton Administration around for at least ten years to work on this. That is good to know.

But the other point would be about this idea of a privacy commission, or whatever it is called, made up of predominantly or entirely of private sector members who are unpaid but perhaps have a paid staff of some sort, whose decisions on matters might be reviewable by courts. The question is: Is there a model like this in the United States in some other area, perhaps a cable board, as an example? How workable is this idea?

Ms. Obuchowski: Well, I think some of the states have privacy councils. They are probably models that go back to the more optimistic days of the late '60s and early '70s, and love beads, and all sorts of things.

Mr. McConnell: They weren't all bad.

Ms. Obuchowski: My husband, Bert Halprin, a Reagan FCC bureau chief, was on the Massachusetts Privacy Council and served proudly. There are some state experiences that might be brought to bear.

Mr. Hammond: Yes. And certainly, the law which we are in the process of developing still can be litigated in the courts. If the cable company decides to challenge, it is going to be refuted. So in that sense, there will be an appeals process. And you can do that.

Mr. McConnell: So there is an administrative appeal first, before you go to litigation.

Mr. Hammond: Right.

Mr. Cate: I wanted to, if we could divert this from privacy—while at the same time promising you, Bruce, which I think I certainly can do, the avid cooperation of all of the panelists here in designing any structure that would deal with privacy issues—to focus more broadly, drawing out the lessons, whatever we can, about the government's role.

One of the topics covered this morning was the question of uncertainty. What role does uncertainty play in the marketplace? What role does uncertainty play in investment, in the willingness to create and deploy new information

technologies? And that would seem to be a feature of the common-law system which was being spoken so warmly of —a guaranteed degree of uncertainty.

On the other hand, there would seem to be at least one strong feature of that. I would think there is some correlation between a common-law, as opposed to a legislative, regulatory system and interest in free expression—interest in the government not setting the terms of speech—but rather playing whatever minimalist or other role it might play in dealing with specific problems that arise. Now, those are clearly two tensions in the common-law debate. Are there other advantages or disadvantages of this? By common law, I take it the opposite of common law is the megamapping of all of the issues in advance, the three times around the wall with all of the issues. Are there other comments that you would like to offer on that?

Mr. Hammond: Well, you don't know if that approach is going to work. In terms of the amount of uncertainty, whenever the technology changes, the government, the public, and industry have a great opportunity and a great problem. The problem is you don't know where things are going to be tomorrow, so it is very difficult to make any long-range prognostications or any prescriptions. But the value is that you get to structure the change on a smaller basis, with a lot of participation, ideally, from everybody who is affected by it. And you come up with something that better approximates what society, industry, and, ideally, the government is seeking to achieve in the first place. I think the common-law approach, in that sense, works very well.

The value of interagency committees and other federal agencies, and previous court decisions is that we don't start on this process as if it just happened today. This has been an ongoing process. You have already talked about what happened in the '60s and the '70s, but it predates even that. There is quite a bit of valuable information that can be generated. There is a history to be looked at, and evaluated, and made a part of the whole process. And there is still the concept of government being more responsive and making its product, in terms of information, more available and more useful to the citizens. And in that sense there is room for both approaches.

Mr. Rotenberg: Let me just say that I like the common law, but I also think that in this area you almost have to be a romantic to believe that it will have a significant impact on the resolution of international telecommunication issues. I like the common law; I mean that seriously. I thought Judge Leisure's *Cubby* decision,(33)—one of the real cyberspace opinions out there—was very helpful to understand some of the information-related issues.

But I can't begin to believe that this particular case is going to have much of an impact on the issues facing the United States, Europe, and East Asia regarding the liability of telecommunication carriers for the content of their networks. And, for that reason, we are going to have to wake up to the reality of the complexity and the global nature of the systems that we are building and try to find the roles that are appropriate.

Now, it is not surprising that principles—principles of the development of the NII, or recast as principles in the development of the GII—have moved to center stage in this policy arena. Principles are very useful as a nonjargon, general-purpose way of stating succinctly what your goals are. It was very interesting, for example, when the United States came to the meeting in Brussels last week. We had five principles for the GII. I think the European contingent maybe had eight. In any case, there was an agreement on a principle—some expansion. I have been following these principles since they first were announced by the Vice-President. Originally, the Vice-President had nine principles but then along came the budget cuts, so he cut them down to only five.

This is a good area to have public discussion about goals and about aims, but I don't think it goes far enough in terms of providing safeguards and protections. The common-law cases will give us interesting insights. When a judge looks at a situation and says, "This is the right way to do this," you learn from that experience. But I'm afraid that process is just too slow for the age we live in.

Adrian Cronauer:(34) I would like to go back to the privacy issue for just a moment. Rich's comment about the cellular, the comment about Bork, and the business about Caller I.D. all point out that much of it is a matter of managing expectations.

I happened to be living in Philadelphia when this whole business came out about Caller I.D. a few years ago and was soundly treated in the opinion columns and on talk radio. It occurred to me at the time that had Bell originally invented

a machine that would identify the caller, the entire telephone structure would have developed just as well and just as pervasively, and no one would have worried a bit about it. It would have been expected. But the perception was that this was something that could not be done. And when people realized it could, then the problem developed. Similarly, much of the shock from the Bork videotape event came from the fact that people never realized you could extract information like your video rental records.

Perhaps much of the problem is the disparity between public perceptions of what is and is not possible and of what can be expected by way of protection of your own privacy, whatever that means. Some might be better than trying to play regulatory catch-up, which eventually leads to a regulatory rule that continually grows. Perhaps this would be the better solution in dealing with the whole problem. Just manage expectations. What do you think?

Mr. Hammond: Well, you could try to manage expectations, but if you don't know what the technology can do, you can't possibly alert people to what it's going to do for them. We only know what it can do today. Take video transmission as an example. Knowing that six megahertz of spectrum would allow us to transmit a video signal would not let us know that if we got into compression we could transmit data. Knowing that we could transmit data we could not know we could send a message to someone on the other side of the United States and have it show up on our watch. We couldn't know.

So we can inform the public to a certain extent. We can inform the public as quickly as we know; we can even tell them what we expect to occur. In fact, we have been seeing and doing a lot of that over the last four or five years with this NII and GII. There is just a limit to what we are able to anticipate before some engineer, some laboratory, some enterprising consumer, or some business person says, "Well, wait a minute. If I look at it this way, I can do something different."

Mr. Rotenberg: I think, actually, Thomas Edison had a very wise insight about this problem. He said, "What man creates with his hands, he should control with his head." I think to ask the policy question, "Just because we can do something, should we do it?"

Tony Amsterdam, a professor at NYU, wrote twenty years ago about the expectation of privacy problems. He wrote that the government could say tomorrow, "You have no privacy. We intend to gather whatever data we can."(35) Would it be better, with the notice, when our expectation of privacy dropped to zero? I think the answer, of course, is no.

The approach that has been taken—in contrast to the common-law approach on the privacy front—is to say we do want an expectation of privacy in financial records, in video records, in medical records, and so forth. And we will enforce that expectation through a statutory scheme. That scheme is not an absolute safeguard, but one which makes clear as a general matter that the records will be protected, and that there will only be certain exceptions where they are disclosed.

Once again my theme is kind of getting your hands on the wheel. I think it is very, very important in this area of public policy to have a sense that there are choices to be made about what the goals are and how to proceed towards those goals.

Mr. Cate: Are we headed towards re-regulation, new regulation? The bellwether of the past twelve years was deregulation. When I look at the list of Task Force committees and when I think about the Vice-President standing just across the road at the National Press Club and saying, "The reason the Titanic sank was because there weren't laws requiring communications operators to do certain things, and what we need are some new laws," I can't help but think so. He didn't say some new principles that we could discuss in a public arena; he said some new rules. Is that where we are headed? Rules for universal access, rules for privacy, rules for intellectual property? Is that what we should be expecting? Is that the expectation of this process?

Mr. McConnell: I think the jury is still out on that. I agree with the point Charlie made, that we don't know which of these things would work best. We need to pursue it on all fronts. Certainly, the climate at the moment is not pro-regulatory, so I think we have to take that reality into account as well, no matter what we think is the right approach.

Mr. Cate: Janice, do you have any comment on this? You were certainly part of the deregulatory move.

Ms. Obuchowski: Well, I am not going to sit up here and say the FCC isn't needed any more. Actually, the good news about the Vice-President is that he is a visionary and who only occasionally dabbles in rules. He has been very remarkable in putting over his vision and, as a result, can take justifiable credit in raising the consciousness, almost single-handedly, of Americans at large. He has put these issues on the front page more than any single person, and to my satisfaction, his predilection towards rules has not really gotten off the ground.

In information policy, we probably will get some rules to govern issues, for example, in health records. They probably will be for the good. I don't suspect this area is going to be overregulated, partially because it is so darn complicated. They just don't understand it on Capitol Hill, and they would rather not touch it. Tell me if I am wrong.

Mr. Rotenberg: I agree that today, people are afraid to make mistakes. Senator Exon is afraid to make a mistake with this bill. I think thoughtful people understand the problem. But that, you see, doesn't mean that problems won't arise. And the question will then become, "When those problems arise, how will government respond?" because you can't wish problems away.

However successful particular ventures might be, the concerns of these 13,000 telephone subscribers in Pennsylvania are real concerns. I think what will be happening—and, again, we are not talking this year or even 1996; we are looking five, ten, twenty years in the future to when policymakers will be facing concerns about the issues that we've identified: intellectual property, privacy, and access. These problems will be magnified—magnified by the nature of the technology, magnified by our growing dependence on this new type of economy, magnified by increasing conflict over claims of rights. We are enjoying on the front end of this process, I think, quite a bit of leisure and luxury, kind of picking and choosing, among the issues. I do not think that is going to be the case at all a decade from now.

Donald Haines:(36) Let me suggest that there is a real difference between an emphasis on deregulation and nonregulation, in terms of protection of rights, and a real interest in regulation, if the interest is in terms of curtailment of rights.

The Clinton Administration, for example, had no problem favoring regulation if it was digital telephony. It has no problems favoring regulation if it is the Clipper Chip. It has no problems with Smart licenses from the FAA for pilots, Smart cards for food stamp recipients. In fact, I think the element of unreality that we started out with has sort of wandered into us as we contemplate the global policy issues in the year 2000. The fact is real rights are really at jeopardy now from real actions, from people who are really trying to regulate. So it seems that is where we are.

Mr. McConnell: I think that kind of comment which suggests, for example, that the Clipper is a regulatory initiative, when, in fact, it is not, confuses the issue. There was certainly a lot of discussion within the Administration. We ended up supporting digital telephony, but it was not an easy question. There were long discussions about the balance of interests.

As to the things like Smart cards and databases, I think that we have a real problem. If you take a look at the welfare reform proposal on the Hill right now, there is a big, fat database in there, the new-hire database, which any time anybody gets a job, their name will be put in a database. Well, pretty soon everybody will be in that database, and that is a bipartisan proposal.

So I think there is a lot of education that needs to be done as to the questions of balance, and the differing and varying public interests. In the welfare area, I find it particularly pernicious, because it appears that people who are on welfare don't seem to have any privacy rights. But they are only the first on the list.

Mr. Hammond: Well, there is a quid pro quo for eligibility for certain benefits, which are—that is not a conservative or a liberal response; that is a reality. For those of us who have the option not to use our credit cards, or not to use our ATM cards, and use cash instead, or to not give out that extra piece of information if we use a check in the grocery store, there is a long list. I have friends, who are real "techies," who say, "Look, don't use the system. Don't use the telecommunications network for many things, because you are creating a record every time, and because you are allowing people to invade your privacy as a result, by virtue of the databases that begin to develop."

I think there again, the first issue is education. I think Janice is right. Most people don't understand that they are giving up little bits of their privacy every day, and they won't understand it until either something blows up in their face or they have it explained to them in very basic terms.

The Social Security card is the perfect example. I can't get medical attention without it. I can't apply for credit without it. I can't open a bank account without it. I can't have a job without it. By the time you finish, there is nothing that people will not know about me by virtue of having access to that number. So we have already sort of crossed that threshold for everybody.

Mr. McConnell: And yet the law provides that no federal agency can require you to give that number. So there is a paradox.

Mr. Hammond: Right. That's right. That raises another really important issue. There are some things which are state actions, the state is precluded from doing it. But with large corporations having the same amounts of power that the state has, in some instances, where is the difference?

Mr. Rotenberg: But, again, that is another example of a policy choice. I mean if you are prepared to say, "We have some concerns about the unmandated use of the Social Security number. We recognize that it's in widespread use, and we are about to put together this database," maybe we will decide we want to go forward with this program. But we want to do this in a way to protect privacy, so let's get a number other than the Social Security number for worker identification. And suddenly we begin to realize, maybe we don't have to put consumers in the position of constantly giving up privacy interests to get something they would otherwise need. Maybe we can design systems. Maybe we can develop new business practices that both allow markets to flourish and protect people's privacy.

One of the things I feel very strongly about on this issue is we need to get away from the zero-sum analysis which says if we get privacy, we give up access. If we get privacy, we have less competition. I think we need to find solutions which say we are going to have all these things together, make those our goals, and go toward them.

Mr. Papapavlou: I would like to propose something from the private sector's point of view. There is a point to make that the private sector may have an interest to be more sensitive towards privacy protection. It is a situation we have at least now in Europe—and I think in the United States you probably have it stronger—with environmental protection, whereby those companies who can claim to protect the environment with the products they produce use those as a marketing argument.

I mean there are products which say, "This is a biological product. It is an environment-friendly detergent," or whatever. To do this in the context of privacy, of course, you need sufficient public consciousness of the need to protect privacy. Privacy has become a priority before it can become a marketable good.

What I would like to say, which is something that Marc has said before, is that if you are talking about global networks and global markets, then Europe, the United States, Japan, and the rest of the world has to come closer together. And this, again, is for the good of industry and for the good of business, who will need to know if there's reasonable homogenous legal framework in which it operates. If there are fifty different legal frameworks that have to be taken into account, then the Internet, or whatever, will have little value, because the minute you go from one state to the other, you enter new problems. So I think there has to be an effort to come closer as much as possible.

My final comment is a question concerning law in the United States. Mr. McConnell mentioned and Marc Rotenberg mentioned principles which have been produced for the use of the private sector by the Task Force—am I right, principles? My question is: What makes it that these principles are considered good enough to be proposed to the private sector entirely in the forms of guidelines, but not good enough to be a law?

Mr. McConnell: I think the answer to that is that the principles are general, and perhaps not specific enough to be enforceable, but that they could lead to more specific legislation, that they are the first way of establishing a consensus on the underlying policy, and that the next step might well be laws, if not comprehensive laws then at least laws in specific areas.

Mr. Cate: I have a question for each of you. You have one thing, only one thing, that you can do to improve the policy making arena. This is not to pass laws about privacy. This is one thing you can do to improve the process, the setting in which policy making regarding information takes place. What would the one thing be?

Mr. Hammond: I was afraid you were going to do that. Publicize it. Really publicize it. Make it open to the public.

Mr. Rotenberg: I would like to see the Vice-President hold a one-day open town meeting on the purpose and goals of the information infrastructure, and invite to that meeting a broad cross-section of the American public. I would like to see him hear, from the public, what they think this should be.

Mr. McConnell: I guess I would like to see more use of the technology itself in the policy debate. Perhaps the open town meeting could be expanded to an electronic open meeting with some public access points, so that anyone could participate and, thus, use the technology itself to help us understand better what people are thinking.

Ms. Obuchowski: Limit all Task Force meetings to one hour, open them to the public, and require a concrete output at each meeting.

Mr. Cate: There you have it. My thanks to the panelists, both from this afternoon and from this morning, and to all of the participants in the audience. We are adjourned.

(1)The Clipper Chip is a code-cracking key. The United States government wishes to

crack every code whenever necessary in order to police criminals. *See* Daniel Perl, *Encryption-Software Plan Presented Using `Keys' Held by Escrow Agents*, Wall St. J., Aug. 18, 1995, at A3.

(2)Office of Management and Budget, National Information Infrastructure; Draft

Principles for Providing and Using Personal Information and Commentary, 60 Fed. Reg. 4362-70 (1995).

(3)Adminstrator of Office of Information and Regulatory Affairs, Office of

Management and Budget.

(4)See Anne W. Branscomb, Who Owns Information? (1994).

(5)Information Infrastructure Task Force, Intellectual Property and the

National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (1995).

(6)Id.

(7)Three `Mega Projects,' OMB Proposes New Privacy Policy, Comm. Daily, Apr.

26, 1994, at 1, 1.

(8)The National Information Infrastructure: Agenda For Action, 58 Fed. Reg. 49,025

(Dept. Com. 1993); National Information Infrastructure, 60 Fed. Reg. 14,980 (Exec. Off. Pres. 1995).

(9)Video Privacy Protection Act, 18 U.S.C. § 2710 (1988).

(10)See Clinton Proposes a `Patchwork' Approach to Data Protection, Computer

Fraud & Security Bull., Nov. 1, 1993, *available in* WESTLAW, COMFSBL, 1993 WL 2577047; Robert J. Posch, Jr., *European Privacy Boards Have No Place in Our Free Society*, Direct Marketing, Aug. 1, 1990, at 78.

(11)See Kay McFadden, *Communications Leaders Meet in Cary*, News & Observer,

Dec. 28, 1994, at D1; *NII Advisory Council Has Busy Week in Washington*, Wash. Telecom News, Dec. 5, 1994, *available in* WESTLAW, WATELNWS, 1994 WL 8735747; *Designing Road Map for Data Highway Privacy, Public Access Becomes Issues*, Sacramento Bee, Oct. 26, 1994, at C8; Steve Alexander, *Information Superhighway Will Have to be Private and Secure to Attract Consumers*, Star-Trib. (Minneapolis-St. Paul), Jun. 21, 1994, at 01D.

(12)See Perspective on the National Information Infrastructure: Ensuring Interoperability, Multimedia & Videodisc Monitor, *available in* WESTLAW, MVIDEOMON,

1994 WL 2693475.

(13)S. 1822, 103rd Cong., 2d Sess. (1994).

(14)H.R. 3636, 103rd Cong., 1st Sess. (1993).

(15)S. 652, 104th Cong., 1st Sess. (1995).

(16)Michael L. Rozansky, *Bell Failed to Protect 13,000 Callers' Privacy*, Phila. Inq.,

Mar. 2, 1995, at C1.

(17)Id.

(18)Id. at C8.

(19)Id.

(20)5 U.S.C. § 552a (1974).

(21)U.S. Department of Health, Education, and Welfare, Records,

Computers, and the Rights of Citizens (1973).

(22)Susan E. Fisher, *What do Computers Know About You? Personal Information Too*

Readily Available, PC WK., Feb. 11, 1991, at 156. *See also* Paige Amidon, *Widening Privacy Concerns*, Online, July 1992, at 64, 66-67.

(23)Jim Mansey was at that time the president of Lotus.

(24)See Robert S. Greenberger, *State Department Aides Are Investigated by U.S. for*

Leaking Bush Personnel Files, Wall St. J., Nov. 10, 1993, at A10; Walter Pincus, *State Department to Probe Access to Personnel Files*, Wash. Post, Sept. 3, 1993, at A1; Elaine Sciolino, *2 At State Dept. Are Out Over Files*, N.Y. Times, Nov. 11, 1993, at A24.

(25)5 U.S.C. § 552a (1994).

(26)Principal Administrator and Secretary to the European Union Legal Advisory

Board.

(27)Council Directive of 24 July 1995 on the Protection of Individuals with Regard to

the Processing of Personal Data and on the Free Movement of Such Data (copy on file with the *Federal*

Communications Law Journal).

(28)Ms. Guiton Hill was the director of the U.S. Office of Consumer Affairs. She was

also President Bush's special advisor for consumer affairs.

(29)Partner, Arnold & Porter, Washington D.C.

(30)Privacy Act, *supra* note 25.

(31)Chesapeake & Potomac Tel. Co. v. United States, 830 F. Supp. 909, 932 (E.D.

Va. 1993), *aff'd*, 42 F.3d 181 (4th Cir. 1994), *cert. granted*, 115 S.Ct. 2608 (1995); US West, Inc. v. United States, 855 F. Supp. 1184 (W.D. Wash.), *aff'd*, 48 F.3d 1092 (9th Cir. 1994); Bellsouth Corp. v. United States, 868 F. Supp. 1335 (N.D. Ala. 1994); Ameritech Corp. v. United States, 867 F. Supp. 721 (N.D. Ill. 1994); NYNEX Corp. v. United States, Civ. 93-323-P-C, 1994 WL 779761 (D. Me. Dec. 8, 1994).

(32)Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848

(1986).

(33)Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

(34)Senior Associate, Maloney & Burch, Washington, D.C.

(35)Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev.

349 (1974).

(36)Legislative Council, Washington National Office, American Civil Liberties Union.