PANEL II OF A HEARING OF THE SENATE JUDICIARY COMMITTEE SUBJECT: FISA AMENDMENTS: HOW TO PROTECT AMERICANS' SECURITY AND PRIVACY AND PRESERVE THE RULE OF LAW AND GOVERNMENT ACCOUNTABILITY CHAIRED BY: SENATOR DIANNE FEINSTEIN (D-CA) WITNESSES: EDWARD BLACK, PRESIDENT AND CEO, COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, WASHINGTON, D.C.; PATRICK F. PHILBIN, PARTNER, KIRKLAND & ELLIS, WASHINGTON, D.C.; MORTON H. HALPERIN, DIRECTOR OF U.S. ADVOCACY, OPEN SOCIETY INSTITUTE, WASHINGTON, D.C. LOCATION: ROOM 226 SENATE DIRKSEN OFFICE BUILDING, WASHINGTON, D.C. TIME: 10:00 A.M. EDT DATE: WEDNESDAY, OCTOBER 31, 2007

Copyright (c) 2007 by Federal News Service, Inc., Ste. 500 1000 Vermont Avenue, NW, Washington, DC 20005, USA. Federal News Service is a private firm not affiliated with the federal government. No portion of this transcript may be copied, sold or retransmitted without the written authority of Federal News Service, Inc. Copyright is not claimed as to any part of the original work prepared by a United States government officer or employee as a part of that person's official duties. For information on subscribing to the FNS Internet Service, please visit http://www.fednews.com or call(202)347-1400

SEN. FEINSTEIN: We will move quickly on the next panel. And as they come up I'll introduce them.

Ed Black is the president and CEO of Computer and Communications Industry Association where he previously served as vice president and general counsel. Mr. Black also serves on the State Department's Advisory Committee on International Communications and Information Policy. Mr. Black spent time in the State and Commerce Departments during the 1970s, focusing on a range of issues, including telecommunications and technology policies. He's worked for two members of Congress.

The next person is Patrick Philbin. He currently works at the law firm of Kirkland & Ellis. From 2001 to 2005 Mr. Philbin served in the Department of Justice where he focused on national security, intelligence and terrorism issues. As a deputy assistant attorney general in the Office of Legal Counsel from 2001 to 2003, a critical time, Mr. Philbin advised the attorney general and counseled the president on national security issues. As an associate deputy attorney from '03 to '05, he oversaw and managed national security functions for the department, including applications for electronic surveillance under the Foreign Intelligence Surveillance Act.

Morton Halperin is the director of the United States Advocacy at the Open Society Institute and the executive director of the Open Society Policy Center. Dr. Halperin has served in three administrations with positions in the State Department, the National Security Counsel and the Defense Department. Dr. Halperin has also worked for the American Civil Liberties Union, serving as director of the Center for National Security Studies from 1975 to 1992. He's taught at

several universities including Harvard, Columbia and MIT. He has missed the West Coast in that area.

But we will now proceed. I will ask the panelists, beginning with Mr. Black, to try to confine their remarks to five minutes and then we will follow up in like manner.

Mr. Black.

MR. BLACK: Thank you, Senator Feinstein.

SEN. FEINSTEIN: Thank you.

MR. BLACK: It's a pleasure to be here.

I am Ed Black, president and CEO of the Computer and Communications Industry Association. For 35 years CCIA has consistently promoted innovation and competition through open markets, open systems and open networks. We greatly appreciate the opportunity to discuss the critical intersection of national security law and privacy rights before this committee.

As we all know, the Internet is an unprecedented and unique force for democratic change and socioeconomic progress. Increasingly, our nation's digital economy -- indeed, our global competitiveness -- depends on the dynamism and openness of the Internet. In a digital economy, all information service companies have a custodial role to play regarding two key fundamentals of the Internet: free speech, as protected by the First Amendment; and privacy and security, protected by the Fourth. If the marketplace loses confidence in the security of business and personal transactions online, the entire digital economy could grind to a halt.

We understand our industry's technology and the many ways in which can be used -- and ways it can be misused. In addition to the most obvious domestic benefits, the Internet is a tool for spreading freedom and democracy around the world. Indeed, our government must continue to lead by example in promoting the freedom of ideas and communications that the Internet makes possible. We urge you to ensure that this legislation not weaken the hand of American companies that must contend with escalating demands for censorship and surveillance by foreign secret police around the world.

CCIA supports current legislative efforts to amend FISA to achieve a sound balance between effective terrorist surveillance vital to our national security and constitutional protected rights to privacy and free speech. We want to be good citizens. We do not, however, want to be police agents. In order to do that we need protection not just from third-party liability for acquiescing to proper demands, but protection from improper government pressure or inducements as well. The Senate Intelligence Committee legislation S.2248, while providing some important improvements over the hastily passed Protect America Act, will allow too much surveillance of Americans based on executive certification, without a court order. And disturbingly, the bill provides a retroactive immunity from civil liability from those who may have participating in an illegal program without a full understanding of what conduct is being immunized.

If we continue to make up the rules as we go along, any violation of the Constitute performed to serve a very tempting national security or law enforcement purpose can be rationalized and covered up by retroactive immunity. Retroactive immunity for participating in the recent secret government surveillance program is premature at best. If immunity for past activities is granted prior to full disclosure and accountability, Congress and the public may never understand the real nature of the NSA warrantless wiretapping program. We also believe broad, retroactive immunity would be ill advised in any event, because it would perpetuate uncertainty, confusion and second-guessing in the future. If retroactive immunity is granted in this case, future extra legal requests will be accompanied by a wink and promise of similar immunity after things settle down. The civil litigation should be allowed to proceed, even if major portions of the proceedings need to be held in cam! era and the scope of discovery narrowed, judges -- and to the extent compatible with serious national security concern -- the public should and needs to learn what really happened in these

In conclusion, millions of workers in our industry believe that we are an industry that can be a strong positive force for our society. The underlying desire to facilitate communications, the transfer of information and knowledge, and the building of bridges across cultural boundaries: these are core motivations of people in our industry. These motivations are part of why our industry is successful. The economic rewards can be great but they are as much a consequence as they are a motive.

To sustain this positive force, we must work together to establish processes and protections for private personal and business information that is so critical to the open and free use of the Internet. Our industry needs clear and constitutionally proper ground rules that are only deviated from through well-defined transparent processes. These rules must be straightforward enough to be publicized and understood by U.S. citizens and businesspeople who may be called upon to assist their government in these uncertain times.

Thank you.

cases.

SEN. FEINSTEIN: Thank you, Mr. Black. And thank you for coming so close to the time limit. I appreciate it very much -- excellent testimony, too.

Mr. Philbin.

MR. PHILBIN: Thank you, Madame Chairman.

I'll try to -- thank you, Madame Chair.

I'll try keep on the time limit as well.

I gained experience related to FISA and electronic surveillance during my service at the Department of Justice and learned that intelligence -- electronic surveillance is a vital intelligence tool --

SEN. FEINSTEIN: Pull your mike close so that everyone can hear, please.

MR. PHILBIN: -- a vital intelligence tool. At the same time, it's an intrusive technique that if not constrained and controlled properly can threaten the liberties and privacy of American citizens. Ensuring electronic surveillance remains an agile and adaptable tool, while at the same time protecting liberties, is the challenge Congress faces in amending FISA. In my testimony I'd like to cover three points related to Bill 2248.

First, I want to express support for the provisions in the bill that will allow the executive to target the communications of persons reasonably believed to be overseas without first going to the FISA court. These provisions are consistent with FISA's original purpose and are necessary to ensure that FISA does not fall out of step with changing technology. FISA was not meant to regulate the collection of intelligence on the communications of persons overseas. The changing technology has led to the fact that some communications going through the United States are now under the FISA court jurisdiction. In my view, given changes in technology, a longer term solution to make the application of FISA less dependent on a medium used to carry a communication, such as wire versus radio, and more directly tied to the location of the target is definitely warranted and this provision is a good start in that direction. It appropriately addresses the nation's intelligence ne!

eds, especially during the ongoing conflict with al Qaeda, when speed and flexibility in responding to targeting and tracking of subjects overseas are vital for intelligence success.

Second, I want to express my support for the provisions in the bill that grant immunity to telecommunications against lawsuits based on the carriers alleged participation in intelligence activities involving electronic surveillance authorized by the president. I think that that immunity is warranted for several reasons: First, protecting the carriers who allegedly responded to the government's call for assistant in the wake of the devastating attacks of 9/11 is simply the right thing to do. The allegations here are that in the wake of 9/11, corporations were asked to assist the intelligence community based on a program authorized by the president himself and based on the assurances that the program had been determined to be lawful at the highest levels of the executive branch. Under those circumstances, the corporations should be entitled to rely on those representations and accept the determinations of the government as to the legality of their actions. It!

would be fundamentally unfair, in my view, to simply leave those who relied on representations from the government twisting in the wind. The fundamental notion of fairness here is also rooted in the law. As was mentioned in the earlier session, there is a common law immunity for those who assist a public officer who calls for assistance during a time of crisis. It's the same principle of fairness that applies here.

Second, immunity is appropriate because allowing a suit to proceed would risk leaking sensitive national security information. As the suits progress, they will inevitably risk disclosure of intelligence sources and methods that will damage the national security and the assertion of

state's secret privilege is not a cure all here. If it were a cure all, the litigation would not still be proceeding two years after it was filed. The longer the suits proceed, the more details concerning the ways the intelligence community may seek information from a nation's telecommunications infrastructure will leak. Our enemies are far from stupid. As such information trickles out, they will adapt their communications security to thwart our surveillance measures and valuable intelligence will be lost.

Third, failing to provide immunity to the carriers here would discourage both companies in the communications sector and other corporations from providing assistance in the context of future emergencies. In the continuing conflict with al Qaeda, one of our nation's greatest strategic assets is our private sector and the information it has available to it. Intelligence is vital for success in this conflict, and particularly communications intelligence. If immunity is not provided, however, it is likely that in the future, private sector corporations will prove much more reluctant to provide assistance swiftly and willingly, and critical time obtaining information will be lost. I agree fully with the conclusion in the report -- in the bill from the Senate Select Committee on Intelligence that, quote, "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our nation."

Finally, I disagree with the suggestion made by some that carriers should be forced, through threat of liability, to serve a gatekeeper role to second guess and provide, in essence, oversight on the intelligence gathering decisions of the executive. Communications companies are simply not well positioned to second-guess government decisions regarding the propriety or legality of intelligence activities. I know from experience that the legal questions involved in such matters are highly specialized, extremely difficult, often involve constitutional questions of separation of powers that have never been squarely addressed by the courts and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communication service to the public. Conducting the complete legal analysis, moreover, requires access to facts and intelligence information that is not and should not be fully shared outside the government. We should not adopt!

policies that effectively require private corporations to demand intelligence information from the executive and to conduct their own mini investigations into the propriety of intelligence operations.

At the same time, there must be some mechanism for addressing concerns raised about the intelligence activities at issue. As the committee is likely aware, I am intimately familiar with the legal analysis conducted within the executive branch about debates about that analysis. I can understand that reasonable people want further probing into legal bases for the program. And ensuring that all intelligence activities do strictly adhere to the law is an imperative, but the question of liability for telecommunications carriers is logically and legally distinct from that debate. The mechanism for addressing legal concerns about the intelligence programs is through rigorous oversight within the executive branch and through a joint effort between the executive and Congress to ensure appropriate oversight. The executive and Congress --

SEN. FEINSTEIN: (Off mike.)

MR. PHILBIN: The executive and Congress are the branches charged with that responsibility and private lawsuits are not the best mechanism for providing that oversight.

In conclusion, Madame Chair, I'd just like to note that I agree with the comments that were made earlier that a warrant should not be required from the FISA court for conducting surveillance of a U.S. citizen overseas. That is an expansion of the FISA court's authority that I believe is unwise.

Thank you.

SEN. FEINSTEIN: Dr. Halperin.

MR. HALPERIN: Thank you very much.

I want to note that there are, of course, many other people and many other organizations that are expert on this and have deep concerns about it. And I know it was not possible to have them all as witnesses, but I trust the committee will look at those views as well.

I want to focus on the issue of immunity and the question of sole means, because I think they're very closely related.

The discussion we've had this morning is a logical one, but it totally ignores the history and the legislation that's before us. It ignores the history because we are at exactly the same point when FISA was introduced and I was very much a part of that debate. The phone companies came in in exactly the same way. They were being sued. I had sued them for participating in the wiretap of my tap of my home phone and they said this is unreasonable. We should not be required to second-guess. When we get a request from the government, we should be able to know very clearly what we we're supposed to do. And Congress provided that answer with extraordinary clarity in the FISA legislation. It said if you have a FISA warrant or a certification from the government that the specific provisions of FISA which permit surveillance without a warrant have been met. If you get one of those two things, you must cooperate. And if you get something else, like a certification!

that says the president has decided this lawful without citing a statutory provision, then they were supposed to say no, and they were subject to civil and criminal penalties if they did not --both state and federal civil and criminal penalties.

I think the law was absolutely clear. And so to now say -- to cite the common law rule that you need to cooperate or say it is unreasonable to put phone companies in this position ignores the fact that Congress answered that question with great provision with FISA.

It is also illogical, the argument that's being made, because the argument says we want them to cooperate in the future and therefore we have to give them this immunity. But as the witness from the Justice Department agreed -- and I thought that was very important -- this bill does lay out for the future a scheme which does not require the phone companies to do any of their own analysis or to make their own judgment about what is patriot. Now, paradoxically, it's the same scheme that was in the original FISA, but a little clearer.

And I think there are ways in which you can go beyond the Senate Intelligence Committee bill to make it even clearer that Congress means to say to the phone companies you either have a warrant or you have a certification that a specific provision of FISA where you don't need a warrant is involved. If you get one of those two, you must cooperate and if you do not you may not cooperate.

Now, that's a rule going forward which will lead the phone companies to cooperate, because there's no judgment. So the logic that says we need to give them immunity about the past so that they'll cooperate in the future makes no sense, because we're telling them to cooperate in the future not if they get another plea that the common law requires them to cooperate, but only if the government meets the standards for the certification. So I would urge you to build on what the Senate Intelligence Committee and add to those provisions.

Another very important provision, in my view, is the question of how you avoid them using this when the real interest is a U.S. person. And again, I think we had very important testimony from the Justice Department saying that when a U.S. person becomes of interest to the intelligence community, we need to get a warrant from the FISA court. And we want a warrant because we want all of his conversations. That is the language that's in the House bill. The House bill says that when a person in the United States becomes of -- when a significant reason to do the surveillance is because you want information about a person in the United States, you need to get a warrant from the FISA court. And I would urge you to add that to the bill. It changes nothing. It's exactly the assurance you were given from the Justice Department, but it makes it a statutory requirement and puts the FISA court in the process of making sure that when the purpose is to learn about an American!

-- a person in the United States -- then you need a warrant.

Finally, more generally, I think you do need to give the FISA court some additional leeway so that it can supervise the process. As we heard in one of the exchanges, the way the bill is written, even if the FISA judge decides that the minimization procedures are being violated, there's nothing he can do. Now, I think a judge would say, you know, it doesn't matter. If this is before me, I'm going to decide it. But I think Congress ought to make it absolutely clear that the FISA court has to supervise all of the requirements of the statute. Thank you.

SEN. FEINSTEIN: Thank you all very much.

Dr. Halperin, you speak very quickly and I think very slowly, so we've got a little point here.

In looking at your point on the warrant accompanying the certification with respect to the existing FISA law -- and I'm looking at the law -- it would seem to me if one just added a few words to say that the warrant essentially must accompany -- it is Section 2511(2)(a)ii -- notwithstanding any other law, providers of wire or electronic communications or officers, agents, landlords, custodians, or other persons are authorized to provide information, facilities, or technical -- to persons authorized by law to intercept wire, oral or electronic communications or

to conduct electronic communications as defined, et cetera, only if such provider, it's officers, et cetera, have been provided with a court order directing such assistance.

MR. HALPERIN: Right. Well --

SEN. FEINSTEIN: So we'd only have to add one word "only."

MR. HALPERIN: Well, no --

SEN. FEINSTEIN: Oh?

MR. HALPERIN: Well, I think "only" is implied, but you certainly could add it. But the other change I think you make and need to make -- and it's one of the four I lay out in my testimony is in (b), which talks about a certification as the alternative to the warrant. And it says "that no warrant or no court order is required by law" -- I think you need to say "by this law" -- "and that all statutory requirements of this statute have been met and that the specified assistance is required" so that you make it clear that a certification has to be based on a specific provisions.

For example, you say in an emergency you can go by a certification or for the least -- (my ?) in the original FISA you can go by a certification. So I think with those changes in these words you would eliminate some ambiguity and I suggest specific language in my testimony.

SEN. FEINSTEIN: Thank you.

Mr. Philbin, what do you think of that?

MR. PHILBIN: Madame Chair, I'm not sure responding on the fly that I have a very well thought out response. But it's certainly true that the interaction between 18 USC 2511 in FISA is complex and that is the key for determining how effected any exclusivity provision is going to be, which I understand to be your concern. I think it would be a mistake to change the provision in 2511(a)(2) to restrict the way that the certification immunity there is provided. I think that that's been in the law for a long time. It's been in the law for a long time for a reason.

SEN. FEINSTEIN: Except now this -- the terrorist surveillance program, all of it, is under FISA, you know? And one doesn't know what the court would have done way back when, but it certainly was worth a try, which didn't happen. And it seems to me that what Dr. Halperin has suggested and in a sense, Mr. Black suggested it as well, is really the way to handle this. That the presidential certification doesn't necessarily provide the guarantees to the telecom -- it certainly doesn't this time and I've read it. So therefore, it seems to me the court does provide the guarantee to the telecoms. And the court does provide the guarantee to the individual citizen. So why not do that, because one of the things we're going to try to do, I believe, is put as much of this intelligence -- type of intelligence collection under FISA as possible.

MR. HALPERIN: Could I just say one point? I think --

SEN. FEINSTEIN: Sure.

MR. HALPERIN: I very much agree with that. And that's why I urge you to require that the government get a FISA order before it begins the surveillance authorized by this program. The government has now conceded a major role for the FISA court. And if provided you have an emergency provision, I see no reason why you should not say "Go to the courts first and get this warrant," precisely because it then says to the court -- it says to the provider: there's a warrant you do it; and if there's not warrant you don't do it.

SEN. FEINSTEIN: And the court will give what I call a program warrant.

MR. HALPERIN: Right, exactly.

SEN. FEINSTEIN: So that's what you're looking for. You're looking for the court oversight. And then the court can set the strictures and say, I want you to report to me every three months, every 30 days, whatever it is. But the court then can provide oversight protection. And I don't think it hobbles the executive at all.

MR. HALPERIN: I agree.

SEN. FEINSTEIN: Does anyone differ with that? My time has -- almost run out.

MR. PHILBIN: I think it is certainly an improvement in FISA to ensure that the court can provide programmatic approvals. I don't think -- my personal view is it is impossible to predict now every exigency of the future that may arise. I think the legislative scheme that you're talking about here is limiting the immunities -- to cut down on the immunity in this 2511 provision going forward so that it specifies only a certain certification, the specific certification in FISA -- or something to that effect -- or a court order.

I can see that if the objective is to provide the immunity only where that kind of piece of paper is given that it will achieve that effect. But I don't think that it is possible to predict now every exigency that will arise in the future and say that FISA's going to have all that covered.

SEN. FEINSTEIN: Well, I guess that's where I really disagree with you. I mean, I think we've reached a stage after the Shamrock investigation, the FISA bill, the prohibitions in FISA, the fact that here it happened, the executive made the decision not to go to the court. They didn't go to the court until -- for a substantial period of time. They stopped the program, obviously feeling that it was legally vulnerable, and then they went to the court. And I think that's a big lesson for us in drafting legislation to prevent this from every happening again.

My time is up.

Senator Specter.

SEN. SPECTER: Thank you, Madame Chairwoman.

Mr. Black, I note that worked with Secretary Kissinger during the Nixon administration and I think it may have been about the same time that Mr. Halperin was under surveillance.

So it's --

MR. HALPERIN: I was also working with Mr. Kissinger in the Nixon administration.

MR. BLACK: And I should clarify, I only joined when President Ford took over.

SEN. SPECTER: You were working with Secretary Kissinger too?

MR. HALPERIN: When he was the director of the National Security Council in the first nine months of the Nixon administration.

SEN. SPECTER: Was Mr. Black under surveillance when you worked for Secretary Kissinger?

MR. HALPERIN: I couldn't reveal that.

MR. BLACK: I should clarify: I only joined that administration under President Ford.

SEN. SPECTER: Mr. Black, was Mr. Halperin under surveillance when you worked for Secretary Kissinger?

MR. BLACK: I'm glad to say I worked on nuclear proliferation and other related issues. So I have no idea. But I really only joined following President Nixon's resignation.

SEN. SPECTER: So you enter a general "not guilty" plea?

MR. BLACK: Definitely not guilty.

SEN. SPECTER: Mr. Philbin, why not indemnification?

First, let me congratulate you for standing up, as Mr. Comey lauded your performance under difficult circumstances.

MR. PHILBIN: Thank you, sir.

SEN. SPECTER: That is both commendable and rare. So thank you. But why not indemnification? Will there be realistic losses to the government by these lawsuits, which will be defended by every procedural device known?

MR. PHILBIN: I don't think that the problem with indemnification as a solution is ultimately the payout of money. That's not the concern. The problem with indemnification is the lawsuit still has to proceed with the carrier as defendant. So the carrier is bearing all the burdens of litigation, which are significant.

- SEN. SPECTER: But there's a motion to dismiss on grounds of state secrecy. The carrier never appears.
- MR. PHILBIN: And if state's secrets had really been cure all -- a silver bullet for these cases -- they would be gone by now, I think. I mean, they've been pending for two years.
 - SEN. SPECTER: Well, what's happening with them? Has anybody collected anything?
- MR. PHILBIN: That's part of my point, Senator, is that it's not the money that is really the problem here. It's part of the problem, but it's the burden of the litigation itself. The cost of going through the litigation itself, reputational and other harm to the companies of going through the litigation, and damage to the United States in the form potential leaks of national security information during the litigation.
- SEN. SPECTER: What information is going to be disclosed? We couldn't even get it disclosed to the chairman of the Judiciary Committee.
- MR. PHILBIN: That, Senator, though, is based on a decision of the executive that the executive was in control of. This will be a decision by an Article III judge. And there's one Article III judge that in one of the cases already rejected the assertion of the state's secrets privilege, because a certain amount of what has become known as the terrorist surveillance program was already publicly described.
- SEN. SPECTER: Well, the Article III judges aren't always right. But I think they've traditionally provided a good balance.
 - I only have a minute and 40 seconds left. I want to ask Mr. Halperin a question or two.
- Mr. Halperin, what about Article II power? The Foreign Intelligence Surveillance Act provide the exclusive remedy, but doesn't the president have Article II power, as the circuit courts have said, weighing the national security interests versus the invasion of privacy that supersedes the statute?
- MR. HALPERIN: Almost -- first of all, almost all of the circuit court decision are pre-FISA decisions and held that in the -- SEN. SPECTER: Almost all, but not all.
- MR. HALPERIN: Not all of them, but there are one or two in the other direction as well. So I think the Supreme Court has never spoken on this nor come close to speaking on this question. But I think --
- SEN. SPECTER: I'm not talking about the Supreme Court speaking. I'm asking you to speak. Isn't this under Article II power?
- MR. HALPERIN: I think there may be some extreme power in some extraordinary situation when the country is directly under attack for the president to act. And I don't think you

can take -- as you say and the Senate Intelligence Committee says -- whatever power there is you can't take away and nor can any president promise that future presidents won't claim it. But what I think the Congress clearly has the right to do is to legislate the rules of the service providers.

I think you can lawfully tell a service provider that you cooperate with a warrant or the certification provided by this statute or the federal government or the state government can put you in prison.

SEN. SPECTER: Mr. Halperin, I have only 13 seconds --

MR. HALPERIN: I'm sorry.

SEN. SPECTER: -- so I'm going to ask you a question before my red light goes off.

You want it limited to counterintelligence only, instead of all foreign information gathering. Why should we try to listen to what Iran is doing about a nuclear weapon?

MR. HALPERIN: We should try to listen to that and we've listened to that under FISA. We listened during the Cold War to the Soviet Union and we had successive directors of Central Intelligence saying "those rules work." There are different problems when you're dealing with terrorists who are trying to conduct operations within the United States. And I think Congress should be open to amendments that respond to the specific problem of terrorists in the United States. But the old rules were good enough for the Soviet Union. I think they should be good enough for information about Iran or other foreign powers.

SEN. SPECTER: Well, I have many more important questions to ask, but I believe in observing the red light.

SEN. FEINSTEIN: Wow!

SEN. SPECTER: And I will say only one thing in conclusion: I regret the ways of the Senate to keep you sitting here for several hours and then only have two of us appear to question. I regret that, but it's a very busy Senate and this happens, regrettably, all the time. So although you have not been treated as you should be, you have not been discriminated against. It happens to everybody on the second panel.

MR. HALPERIN: Thank you.

SEN. FEINSTEIN: I'd like to say thank you. I think your testimony was very important and gave us some good ideas. So thank you very much.

And the hearing is adjourned. (Sounds gavel.)

END.