



Remarks by Homeland Security Secretary Michael Chertoff at Roundtable With Bloggers

Release Date: March 3, 2008

Secretary Chertoff: So, this is the first of what may be a number of these conferences or discussions. So I'll give you kind of a quick overview, and then take questions.

Five year anniversary. There are basically five major bands in which I'll kind of analyze our work: There is keeping bad people out of the country, keeping bad stuff out of the country, protecting the infrastructure, building a capable response agency, and integrating the department.

Let me tell you where I think we are with each of these five where I think we need -- I'd like to just go by the end of the year, so that I can turn the keys over to the next individual with -- in a pretty good functioning car.

Keeping people out that are dangerous: At the ports of entry, we are very significantly ahead of where we were five years ago, and where we were three years ago when I was -- you know, first started here at the department. US-VISIT, two fingers, is up and running at all of our ports of entry. We're now moving to 10 fingers overseas, at the consulates, and here at the airports. That gives us a capability not only to check fingerprints in our existing records, but to check against latent fingerprints that we collect in safehouses or battlefields around the world.

We have an agreement with the Europeans that will enable us to use Passenger Named Record Data, which gives us better information about who's coming into the country, so we can analyze whether there are connections that we need to be worried about so that we maybe take a closer look at somebody when they arrive.

We're getting somewhat more advanced warning of who's getting on the airplane. That, again, eliminates the risk of having to turn a plane around when we discover a "No-Fly" is on the plane when they're coming in here.

When you put all these things together -- tougher documentation requirements at the land border; requiring passports, if you're traveling in the Western Hemisphere by air -- we are strengthening the document requirements, the biometric requirements, and the information that we gather, in order to have a better picture of who ought to go into secondary, and perhaps not be let into the country. And time and again, we have turned people away who you would not want to have in the country based upon what is -- you know, what their connections are, or what their fingerprints turn up on, or something of that sort.

Between the ports of entry, we're on track to build 670 miles of fencing by the end of this year. We are at over 15,400 Border Patrol; that's on track to over 18,000 by the end of the year, which will double the Border Patrol.

SBI net -- which, contrary to Spencer Hsu, is not P-28; I'm going to really spell it out really clearly: P-28 is to SBI net as one cruiser is to the United States Navy. It is not the same thing.

So we have, as of last week, four unmanned aerial vehicles up over the southwest border. We expect by the end of this year to have 40 ground-based radar systems, 7,500 individual sensors. And we do have P-28, which is an integrated approach to radar and cameras, which we've accepted as being functionally workable, and which we're now going to take to 2.0 before we deploy it at other parts of the border. It was never intended to be one-size-fits-all across the border, nor will it be one-size-fits-all across the border. All these tools are going to be deployed in various ways, depending on what the particular topography of the border is.

So I think we've made a lot of progress there, and the results show a decrease in apprehensions, and other metrics that show, in my sense, that the flow across the southwest border is diminishing, although it isn't -- certainly not, by no means, eradicated.

In terms of keeping bad stuff out of the country, five years ago we had zero containers scanned for radiation when they came into the U.S. Now we have almost a hundred percent. We are putting out a new general aviation rule that's going to result in ultimately getting more information about who's flying private planes in

from overseas, and who is -- and what is on those planes, including -- we're ultimately anticipating having screening overseas, before the plane takes off and lands in the continent of the United States, because we don't want people putting a bomb on a plane and then just putting a plane into a building.

We're building a small boats strategy to deal with the possibility of small boats as an attack vector.

Protecting infrastructure. We have our new chemical plant regulations. The most dangerous chemical plants are in the process of being identified, and security plans are being prepared by them for us to review and either accept or reject.

Working with the rail industry, we've dramatically decreased the amount of time that toxic chemicals are held in tank cars is in a stable position. In other words, where they're just left idle. We want to move them; we don't want to have them sitting idly in urban areas or populated areas.

We are beginning our cyber strategy. That will not be done this year, but I'm hoping we can get it, a cyber center, up and running, and have a full set of plans and a funding budget to move forward over the next several years to get to the next level of cyber security.

On response, we've got -- I think FEMA has done a significant job retooling itself: much better capability to track in real time commodities and things that are being provided; moving from a part-time reserve system of disaster assistance employees to a corps of several thousand full-time employees, so they're not -- it's so that it is their day job to be ready and trained to do disaster assistance; much better metrics and computer tracking, with respect to claims that are being received and being paid out in a way that we didn't have three years ago.

And finally, on the issue of integration, much better cost component planning. Metrics, now, they track how we're doing at the border and how we're doing with claims management -- what our flow time is through our ports of entry; what our flow time is through or TSA check points -- all of which makes it easier to manage as a single institution.

Two things remain to be done as the kind of building blocks of maturing the institution. One is to implement the management directive I issued sometime back to drive career progression, so that you have to have joint service, or service in another component, in order to reach the senior levels of the department. That would build the same kind of jointness that you have in DOD.

The last one is to get a campus. We've put it in the budget again this year. I read somewhere, and this may be incorrect, that there is as many 90 individual locations around the greater Washington area, in which various elements of DHS are housed. We've got to have a place where the leadership can be operating in a single office the way it is with most other -- with all other departments. That is important for morale, it makes it easier to manage, and it saves time.

So that's kind of an overview. Things I want to get done I've kind of mentioned. I want to get the general aviation piece done; I want to get REAL ID, and enhanced driver's licenses -- continue to build momentum on that; I want to get the cyber piece planned and the funding stream put out there. Those are some of the major things I want to get done before the end of the year.

Question: Mr. Secretary, you had, at the very beginning, laid out some great progress that's been made in terms of preventing bad people from getting in. And part of the Homeland Security mission, which is a challenging one, is that while you are responsible for protecting against bad things, you're also responsible for facilitating good things. And be that the flow of people, in this case, USCIS is responsible for that for the department. They've begun a \$3.5 billion transformation.

And I'm hoping you could speak to that in two ways. What's your concept of success in that, in terms of the national security part of it, the operational excellence part of it, and customer service part of it?

Secretary Chertoff: Three -- two main things. One is, we have to move from a paper-based system to a totally electronically-based system. We still have too much paper, and it's hard to track, it's hard to manage, and it takes a lot of time.

The second piece is, I want to rebuild -- re-engineer the system in a couple of ways. One is, and the most urgent, is to deal with the background check problem. It just takes way too long for the Bureau to complete background checks for a small but a significant number of people. The majority of people -- you know, if the name doesn't pop up on anything in the -- it's pretty quick. But for a small number -- but still significant, and

certainly to the individual, significant -- if their name crops up and it's an older case, and it's in a file somewhere, someone has got to hunt it down. And to be perfectly honest, that is not a top-priority job for an agent, is to go through an old paper record sitting in a warehouse.

Looking forward as we go electronically, and as the Bureau goes electronically, that problem will diminish. But looking backwards we have to re-engineer the system to be a little tougher. And one of the things we did, for example, with the green cards was we said, for background checks that took longer than six months, we would give you a green card, and then if it turned out the background check later revealed a problem, we would take the green card away.

Now why did we do that -- because I got criticized, "Oh, you're sacrificing national security." Here's why. First of all, if you haven't been -- if it's going to take longer than six months, it's clear that you're not on a Terrorist Watch List, you haven't been convicted of a crime, you haven't been indicted for a crime. In other words, most of the major things you would worry about -- it's a very easy thing to determine whether you've had a problem or not. What you're not going to get in that six months is the guy whose name came up in a file somewhere. And the vast majority of those are benign mentions.

Secondly, you're here. If you're going to do something bad, you're still here legally. The green card -- it's not like we're bringing you in from overseas. So if you think about it logically, the risk of giving you the green card with the understanding that it can be pulled away if something turns up, it's a minimal risk. It's a minimal, marginal risk. Whereas the customer service value of giving someone the green card is high. That's an example of trying to be more cost-benefit in the system.

Question: On the Al Capone style method of pursuing terrorism-related cases on the Visa Waiver program, Friday we held a session on cyber security, and that followed the day after the hearing by the House Homeland Security on cyber initiative. And committee members were critical of cyber initiative, and very concerned about the implementation of that. What can you do to address the committee's concerns about cyber security, and do you have any comments on the stories about the DNI pursuing -- trying to gather some intelligence on web-gaming through a new initiative?

Secretary Chertoff: The DNI and I ought to talk about his initiatives.

In terms of cyber security, you know, we came -- a lot of it's classified, and so -- and the hearing you're talking about was an open hearing. I mean, I've been in a couple of classified hearings where we've talked about this with the intelligence committee, and we've had some briefings, classified briefings, with members of the Homeland Committees and other committees.

The basic proposition with cyber is this: We're nibbling at the edges now, and we need to have kind of a game-changing approach to this. And part of that game-changing approach is to rationalize what we're doing in the federal domain, and get better control of what enters the federal domain so we can determine whether it's a threat or not.

We came -- you know, we are -- there are a series of plans we are developing to get this thing done. We came early to Congress; we came before the plans were developed. Why did we do that? Because when we go to Congress after the plans are developed, here's what I hear: "Why do you wait until the plans are developed? You don't consult with us." Now we go and we say, "Well, we want to consult with you while we're in the early stages," they go, "How come you don't have a plan yet?" That falls in the category of "got you coming and going." You can't win. If you do X, we yell at you. If you don't do X, we yell at you.

I still think it's the right way to do it. We've told them there's an issue here, here's a general sense of how we want to proceed with it; we acknowledge there's more work to be done. It's a hard problem, particularly in the private sector, because the private sector we can only work in partnership with. We don't want to mandate that the private sector do something. We don't want to suggest that we're going to sit on the Internet over everybody and monitor what they do. That would get people's hackles raised. We need to figure out a way to give the private sector the opportunity to partner with the federal government -- but not make them do it. And so it's a very tricky issue.

One of the reasons, honestly, it hasn't been addressed aptly in the last five years is because it's very hard. It's hard conceptually to figure out how best to do it, and it's hard politically because as soon as you talk about the government and the Internet, you really send some people into orbit. So there's been a tendency to avoid the issue, because it's just hard; let's not think about it.

But I think we all collectively agreed, and certainly the President, I think, has this view, that our job is not to avoid hard problems; it's to tackle them. And it is hard. It's going to be tough to design this. But there's no reason to delay the beginning of the process. And so we're going -- you know, we've kind of, you know, got to Congress early in the process, and I hope that they proceed in the same spirit; they recognize that we're giving them opportunity to have input. Input means not just saying no to everything, but also means, have a constructive -- if you have an alternative solution, we're all ears. But just saying that's not -- you know, the super Goldilocks approach, "The porridge is always too hot or too cold," does -- it's not constructive. What's constructive is, "Okay, here's a better way to do that." And, you know, if you have a better way, God bless you. We'll certainly listen.

Question: Is it fair to say that cyber security is -- that that whole area is far behind -- that DHS has been far behind on cyber security --

Secretary Chertoff: I would say it's the one area in which I feel we've been behind where I would like to be. That's fair to say -- which is why we're trying to really grab it.

Question: Mr. Secretary, to follow up on that, my -- I asked my readers what questions to ask, and they focused a little bit on the new cyber security initiative, because there was -- I don't know if you saw the profile of DNI McConnell in The New Yorker; one of his aides told The New Yorker that the cyber security initiative would mean giving the government the authority to examine basically any packet on the Internet.

Secretary Chertoff: Yes, that's just wrong.

Question: Okay. So, for you, what is the -- what are the main threats that you think that, you know, on the Internet, that Homeland Security has a role in --

Secretary Chertoff: I mean, the biggest role we have is to deal with protecting the federal domain; I mean, non-military. We have statutory authority and responsibility to do that. We do some of this with EINSTEIN -- what I call EINSTEIN 1.0, which is kind of a first cut at a system of detection. But for a number of reasons, it's not as capable as it could be. Part of that is we've deliberately not taken the next step -- taken it up to the next level. Part of it is that not all of the component agencies, all of which run their own cyber shops, not all of them have the same level of capabilities; they're not -- they don't have emergency watches up 24/7.

So I think the minimal thing we need to do is get our own house in order, federally. And that means herding all the different cats of the executive branch agencies into a kind of a single pen where we can have some capability of detecting what's coming in and out of the federal domain.

Question: Mr. Secretary, I've interviewed you before about the unilateral things you've done with the environment, as well as the travel initiatives. And before you came in, he was telling us a lot about the bureaucratic oversight that you're having difficulty with. So kind of a two-part question. The first part: Are you happy with those actions you've taken --

Secretary Chertoff: Yes.

Question: -- and have those pandered out? And what is the role for congressional oversight, and how do you think that should be streamlined?

Secretary Chertoff: You see, I think congressional oversight is a very helpful and very good thing and appropriate, and I have nothing but good things to say about it. But it needs to be rationalized. I've heard estimates -- 86 to 88 different committees or sub-committees that supervise our activity.

In the main, what I would like to see happen is, we have two authorizing committees and two appropriating committees; one in the Senate and one in the House. They should own responsibility for oversight. We work well with them. They don't always agree with me, I don't always agree with them, but we work constructively. And at least they have the big picture of what we do. And so when they propose things or they deal with us, they have a sense of what the full menu of challenges we have is.

The danger with having a lot of other committees is this: not just that we have to write more reports or testify more, but that committees -- additional committees, they have a jurisdiction over a little narrow slice of the Department, and their agenda becomes promoting that slice. And they don't have the visibility into the trade-offs that are involved. So you wind up getting a lot of conflicting direction. This committee is concerned about this problem, that committee is concerned about that problem -- and they want their problem attended to. And

you can't satisfy a hundred masters.

So if Congress could funnel these things through, like most departments, to -- you know, each House has one authorizer and one appropriator -- then I think we'd have a good balance. Congress could certainly do oversight and -- but at least it would come through a perspective that sees the whole range of what our issues are, as opposed to simply one issue.

Question: Do you have any idea how many times you've testified before Congress? I mean, I know it seems like every other week.

Secretary Chertoff: I don't -- I actually do not wind up testifying all that much. I probably testified less than 10 times a year. But the Department testifies a lot, and we do a lot of briefings, and a lot of requests for information. We do hundreds and hundreds of reports. That's where the real burden comes in.

Question: Okay, one last question, sorry. I didn't realize that you were housed in 90 different sites.

Secretary Chertoff: I figure 90 -- but a lot.

Question: Okay, something like that. What else would you propose that Congress do, just to make the functionality of the Department work better?

Secretary Chertoff: I think consolidating us; I think funding our budget requests for the not-particularly-glamorous-but-indispensable things having to do with management, acquisition capability, IT capability. You know, this is stuff which -- you know, when they're trying to make the budget at the end, and often, in order to have more money for grants, they cut that stuff. And the problem is when you cut that stuff, invariably what happens is, six months later, we get a criticism for, we're not managing our acquisitions well. Well, you can't manage your acquisitions well if you can't hire people to do it.

So I'd like to have a balanced program of funding, and I think that -- you know, and I think our budget requests does that -- I think that, plus our getting into a single campus, would be very, very big steps forward.

Question: Sir, when you came onboard, you immediately started talking about risk, and how risk analysis and risk management would play a role in how resources were put out, how firms would run, et cetera. And you mentioned the chemical area earlier, as to what was working there. It seems, though, that there aren't necessarily commonalities to risk on how we're looking at different infrastructures. And how can we give this President and his successor a really good -- I would say, a really good map of where we are with risk in this country, when all the various infrastructure pieces that we've got, those puzzle pieces don't match up by how we're looking at risk?

Secretary Chertoff: Well, I think for us they do in this sense. We generally look at risk as consequence, vulnerability, and threat -- and threat includes intent and capability. And of those things, probably the most significant is consequence, because it's the least variable. I mean, threat, in terms of intent and capability, can change quite readily. Vulnerability, if we're doing our job right, gets reduced -- so that should be a risk reducer. But consequence, really, generally means the same. And that's the template we use across everything.

So we use that with -- and the other technique we use is, we tend to be performance standard-based as opposed to specification-based. And I will say, to reduce the risk, you've got to be able to do the following things, and we talk about outcomes, like: defend against this kind of attack for this period of time; or, in the cases of the railroads, reduce the percentage of stationary dwell time in a population area by, let's say, 75 percent. And that's all funneled under this notion if you reduce the vulnerability, that's reducing the risk because if the consequence stays the same, and the threat stays the same, you've at least -- you know, they're all multiplied by each other. So I think that we actually do use that formula.

Now, others, of course -- the states and localities -- measure things a little differently. When individuals look at risk, or individual communities look at risk, they look at their own risk. They don't trade off against somebody else's risk. So sometimes you get -- that's why you get a lot of criticism from local or state officials, because from their perspective, we're not seeing their risk, and they're not paying attention to the risk of other communities. So when we get into the big city -- you know, the urban grants -- everybody always feels they're getting too little. But we have to look at the whole menu across the board.

Question: Mr. Secretary, if I may --

Secretary Chertoff: I want to make sure everybody has a chance --

Question: The debate in Congress this week, as it's been for much of the past three months, is about the reauthorization of FISA, and the debate over -- especially from the telecom community. Can you provide any kind of categorical statement as to whether ICE agents, CBP agents, have had to drop investigations, or if there has been a loss of information about new terrorism groups since the law expired?

Secretary Chertoff: Well, unless our agents are operating through a JTTF, we don't usually have FISA coverage. You know, ICE and CBP in its normal course, it is not dealing directly with FISA. Now we may get -- you know, intelligence information may come to me that will include FISA stuff, but it's not necessarily going to be something that you could say a CBP or an ICE investigation was based on that, except insofar as part of the JTTF. Look, more generally, I think that we need to get this up and running for reasons the DNI can speak to much more specifically and authoritatively than I can.

And the one issue on retroactive liability, it's just kind of a simple proposition, which I'll come to you at not as a -- in my current job, but just having been a lawyer for a long time and having been a judge. If you punish people for helping the government in good faith, you will not get that help in the future. And some day a President -- there's going to be an unintended thing, and a President is going to need to go to somebody in the private sector and say, "This is an emergency; help me out." And you would not want to be in the circumstance where the person says, "No, I want to have -- I'm not going to do it because I'm afraid I'm going to get sued."

That's why we have, for example -- I'll give you an example -- that's why we have such a thing as congressional immunity. Why is there a speech and debate clause that the Constitution has that allows a member of Congress to get up, if he wants, and literally defame an individual maliciously -- it could be done -- and is protected against being sued? It's because the recognition by the framers was that in order to allow the system as a whole to work, you have to tolerate the fact there may be some bad behavior, because it's important to protect the ability to make those kinds of statements.

That principle of immunity -- judges get it, prosecutors get it. I think there's a reason for that. And it does mean that sometimes, you know, someone can't be sued for something that they do that's wrong, but it's designed so that the system isn't constantly being gummed up because lawyers have to, you know, say time out, and then write opinions and, you know, people become risk-averse.

Question: Okay, just to follow up, you haven't asked -- you wouldn't normally find out whether those investigations have been halted or --

Secretary Chertoff: It would be hard for me, because I don't get a direct visibility. I get the product. I don't -- I'm not involved in the collection.

Question: I want to clarify this relationship with NSA. So you get -- in what form do you get NSA-intercept information? Then, where does it go? How do you use it?

Secretary Chertoff: If we get intelligence, we get it from all over the intelligence community. It can be in -- largely, it's analytic stuff; stuff that has been analyzed and, you know, viewed by the NCTC, or something of that sort. And if we're talking about -- let me step back.

Question: I'm talking directly -- specifically about NSA.

Secretary Chertoff: All right, so let me tell you. In terms of FISA stuff, or things of that sort, we don't operate FISA. We don't do FISA wiretaps in our department. So we do not collect any signals information under FISA or under NSA-type authorities.

All we get is product. We may get product that is incorporated in analysis, and we may not know exactly what the source of each is, or it may be generically described. In some circumstances, if it's relevant, I may get a fragment or an excerpt or a summary -- probably a summary -- of something that's intercepted through FISA or through, you know, some other type of capability.

Question: In that case, you would say, okay, this needs to go to Border Patrol.

Secretary Chertoff: In that case, depending on what it is, you know, we would say, okay -- if it suggested, for example, that there's going to be an effort to smuggle a bomb in through a container, it would cause us then to make some adjustments at the port in order to prevent this kind of thing from happening.

Question: And then would this information be labeled as coming from NSA?

Secretary Chertoff: Not necessarily.

Question: But it could be.

Secretary Chertoff: Could be.

Question: And so therefore you would have been a recipient of, and a user of, information collected by NSA without a warrant.

Secretary Chertoff: Well, it depends whether it needed a warrant or not. I mean --

Question: I'm talking about, say, with the telecoms.

Secretary Chertoff: I'm not going to speculate where it comes from. I can tell you, stuff comes from various intelligence --

Question: Well, you already said it comes from NSA.

Secretary Chertoff: Yes, but that doesn't mean it was done without a warrant. It might have been done with a warrant; it might not have been done with a warrant. It might have required a warrant --

Question: So you don't know if it was done with a warrant or not?

Secretary Chertoff: Right. I would have no visibility into what the legal requirement was, whether a warrant was obtained, whether a warrant was necessary. None of that is visible to me, or revealed to me.

Question: But you are aware --

Moderator: We're tight on time --

Question: I have to finish this --

Secretary Chertoff: I was aware of what?

Question: Were you aware that this program was ongoing with the telecom companies?

Secretary Chertoff: I don't know what program you're talking about.

Question: I'm talking about harvesting information --

Secretary Chertoff: I'm not -- but you see, you're assuming stuff you've read in the paper.

Question: I'm not. I'm asking you for information.

Secretary Chertoff: I'm telling you I have received -- we get information from the intelligence community. It can be collected from a variety of sources. I don't know which program it comes under. I don't know whether it's got a warrant or doesn't have a warrant. I don't know whether it's collected -- I mean, as soon as I can contextually tell where it's collected or not collected.

So I don't know if it's under this program or that program. None of that is known to me. All I know is, incorporated in the massive intelligence we get is all these different streams of intelligence, which help us decide whether we need to do something to protect the country or not. I can't verify your assumptions concerning whether something was under this program or that program. I have no basis to accept your characterization of harvesting, which doesn't strike me as having any legal significance.

So there's a whole bunch of assumptions I want to be clear I'm not buying into. I'm only telling you we had to try --

Moderator: We've got to go to the last question, I'm sorry.

Secretary Chertoff: No. Finish the thing.

Question: Well, you're redefining what I'm saying. I'm not making any assumptions whatsoever.

Secretary Chertoff: I'm only telling you, we get --

Question: The administration, as far as I know, has conceded that information was gathered from wiretaps on telephone companies. Otherwise, why would they be asking for immunity for these companies, right?

Secretary Chertoff: I would not necessarily know --

Question: So if you have -- if you received NSA information -- I'm merely asking if you received information during this time period from NSA -- like you said, we get a bit of a piece of information and we might give it to, say, border control or port security, whatever. Therefore, is it safe to assume, whether you knew it or not, that you would have gotten information from this program? Or are you saying, I don't know, I wouldn't know?

Secretary Chertoff: I don't know. It's not safe to assume, because I don't know. Because I -- because it doesn't come labeled as the particular source. So it would be a guess.

Question: One of the things that I'm curious about is, we're talking about airlines, who's getting on the planes, and so forth. To what extent do you think that it might actually be more efficient to, say, have security on these airlines being dealt with by the companies themselves that run the airlines rather than have it centralized under Homeland Security?

Secretary Chertoff: So that private companies would have all the intelligence and would use it for commercial purposes?

Question: No, no, no, I'm talking about screening passengers as they're getting onto the plane; I'm talking about that. I'm talking about, like, looking at the --

Secretary Chertoff: Well, here's the deal. We tried the private sector screening approach and the company that did it was indicted once, and then when I was head of the criminal division, we indicted them a second time because they hadn't learned the lesson from the first time. So, fool me once, shame on you; fool me twice, shame on you; fool me three times, shame on me.

Question: Wow, you got that right.

Secretary Chertoff: I don't think there's any reason to -- that we even want to entrust -- I mean, they do -- they're certainly welcome and should do screening themselves, for their own purposes, but in terms of deciding who should be admitted into the country and screening for purposes of knowing whether someone is --

Question: That's not what I'm talking about.

Secretary Chertoff: Well, what are you talking about?

Question: I'm talking about getting onto the plane.

Secretary Chertoff: You mean instead of TSA?

Question: Yes.

Secretary Chertoff: I have no reason to believe that the airline -- first of all, the airlines were never in that business, nor do I think they want to be in that business. There were private companies that were in the business that did a woefully poor job prior to 9/11. And we have actually offered the private sector the option of doing private companies in some airports, and, frankly, there's been very little interest. They do it in a couple of airports; I think San Francisco does it. It is not -- there's not been a widespread clamor to do it.

Question: Do you think that that's because they think that the government is better at it or do you think that they're just trying to avoid getting any blame in case something happens?

Secretary Chertoff: I'm sure the latter. I expect that the latter as is probably -- it's not a moneymaker for them. It's not a big -- and nor is it, frankly, to be honest, part of their core expertise, so I can't -- I'm not blaming them, but it's not -- I'm sure if it was -- but I'm sure liability issues play a role in it. There's probably a whole lot of things.

All right, thanks a lot.

###

This page was last reviewed/modified on March 3, 2008.