THE BROOKINGS INSTITUTION

A Brookings Briefing

OFFSHORING AND PRIVACY:

CONSUMER DATA IN THE GLOBAL ECONOMY

Friday, April 8, 2005
10:00 a.m. - 11:30 a.m.

Falk Auditorium
The Brookings Institution
1775 Massachusetts Avenue, N.W.
Washington, D.C.

[TRANSCRIPT PREPARED FROM A TAPE RECORDING.]

A G E N D A

Moderator:

Lael Brainard, Director, Poverty and Global Economy Initiative,
The Brookings Institution

Panelists:

Daniel W. Caprio, Jr., Deputy Assistant Secretary for Technology Policy
and Chief Privacy Officer, U.S. Department of Commerce

Kiran Karnik, President, National Association of Software and Service Companies

Evan Hendricks, Editor, Privacy Times

Jeff Lande, Senior Vice President, Information Technology Association
of America

P R O C E E D I N G S

MS. BRAINARD: All right. Good morning. I think we'll get started. Thank you, all, for coming this morning, on this beautiful spring day, and lots of sunshine.

We have actually wanted to do this event here at Brookings for some time because this issue seems like one where there's a lot of heat, but not a lot of light, as is true of much of the offshoring debate. It is I think probably one of the most important issues in the offshoring debate. I think there's been a lot of discussion about the jobs aspects, the competitiveness aspects, but less in-depth consideration of whether there are risks associated with offshoring over and above the kinds of risks that we had even in the domestic market on consumer privacy issues, on data security issues, and then questions about whether we have just about the right regulatory framework right now or whether, in fact, there are holes--what kinds of initiatives there are out there that might be most productive in actually addressing the privacy issues as opposed to very broad brush approaches that might cut off this source of international trade altogether.

So, today, we have I think a very balanced panel, and also a very knowledgeable panel, and what I'd like to do is have a discussion really where I'll ask each of the panelists to spend a few minutes talking about what they see as the framework that's out there, how adequate it is, what risks we really need to worry about, and what kinds of measures are under consideration or should be to address them. And then what I'd like to do is open it up to the audience to have that discussion.

So let me start with Dan Caprio, to my left, who was kind enough to join us today from the Bush Administration, where I'm sure his job is more than 24/7. So thank you very much for finding the time.

Dan Caprio is currently the Deputy Assistant Secretary for Technology Policy and the Chief Privacy Officer for the Department of Commerce, which, as you can imagine, is a huge job these days. He has been in that position for about two years now? And in that position, he oversees all the Department of Commerce's activities related to the implementation and development of federal privacy laws, policies, and practices at the same time as his group tries to make sure that our economy and the technology component of our economy is competitive as they possibly can be.

Prior to that, he worked with Federal Trade Commissioner, Orson Swindal. And prior to that with a group of experts at the OECD also looking at these issues, and the FTC obviously has a big jurisdiction on some of these issues.

So what I'd like to do if I could is ask you talk a little bit about what is the current regulatory and legal framework and how adequate is it, where are the holes, what are you at the Department of Commerce actively worried about and working on?

MR. CAPRIO: Sure. Well, thanks, Lael. And thanks to Brookings for having this forum. It's not often that I get to sit on the left, but it's--especially with my good friend, Evan Hendricks--but here we are. So.

But yeah, thanks for the opportunity. You know, obviously as companies expand, as U.S. companies expand into international markets, the issue of cross border data flows become more common, and the need to reconcile the requirement for adequate consumer privacy standards and the need for developing flexibility in developing those standards, you know, must and it needs to be addressed.

In general, I mean we're all familiar with the regulatory framework that we have in the U.S. of flexible regulation, backed up by--you know, flexible for--of medical--I mean we

have statutory provisions for medical and financial and children's, backed up by strong law enforcement at the FTC and Department of Justice.

But it's our experience at the Department of Commerce that self-regulatory initiatives, coupled with that government enforcement, provides the backstop, along with the sector-specific legislation, as the most effective way to achieve the meaningful privacy policies and regulations that we all seek.

The examples of some of those self-regulatory initiatives that have been successful include company codes of conduct, the seal programs like Trustee, BBB on line, alternative dispute resolution mechanisms and the like.

It's important that privacy standards ensure a satisfactory level of consumer privacy without negatively impacting the free flow of commerce, electronic commerce and the cross border trade in goods and services. International commerce requires the necessary flexibility to develop privacy protection measures, tailored to the particular needs of the sectors, customers, and employees.

India provides a good example as an example of the confluence of consumer and business needs. In, you know, the country of India, India has a thriving IT-enabled service industry just as the U.S. does that relies on cross-border data flows, you know, with the rest of the world.

At the Department of Commerce, we've been engaged, through the India high tech cooperation group, the HTCG--our last meeting was in November of 2004, and we've got a meeting coming up again in just a couple weeks--I think April 19th.

But that's been a very constructive framework for Indian and U.S. businesses and our two governments to be able to have a dialogue, a very constructive dialogue on the issue of data privacy.

Mentioning touchstones in data privacy, I should mention the European Union, the safe harbor program, which went in effect in November of 2001. That framework with the EU enable U.S. organizations to be able to comply with the data directive and to continue transfer of transatlantic data. And that obviously--the framework--stems from the data directive, a conference of EU law, that could have interrupted the transfer of that personal information.

As of March 1st, the safe harbor has approximately 700 organizations, including Microsoft, Disney, Continental, Boeing, Amazon, Caterpillar and the like . So, you know, a number of leading companies in that 700 continues to grow.

At the Department of Commerce--and, you know, within the Administration--we understand the concerns and agree that protecting privacy and security of personal information collected by U.S. companies is important with respect to--and this is an issue I think we'll get into later--but with respect to the extraterritorial application of U.S. privacy protections, we've been advised, and I think you're probably familiar with this, but that the Federal Trade Commission last spring articulated its position that we agree with that a company that's subject to U.S. privacy laws must take reasonable steps to ensure that that information shared with its service providers, whether domestic or foreign, is protected in accordance with those laws, and so that extends to--we can get into this a little more deeply later--but, you know, in some instances the Fair Credit Reporting Act, the COPPA [ph.] Gramm-Leach Bliley , so that if information--

MS. BRAINARD: Can you just--since not everybody is going to be at the same level of expertise, and I certainly am not. For each of those statutes, could you just describe them real briefly?

MR. CAPRIO: Well, Gramm-Leach Bliley was the statute that was passed in 1999 to protect financial information and has a number of components underneath that, including the safeguards rule for how data is secured and managed.

COPPA is the Children's Online Privacy Protection Act, which was passed maybe a year or so earlier--'97, '98. That protects the collection--protects children online, children under the age of 13. And then, of course, the Fair Credit Report Act, FCRA, which was just reauthorized and preempted two years ago, that's the--that statute goes back to I think 1970, and that's what governs our--the credit reporting agencies and the way information is collected and then disseminated at the back end. But, you know, it affords--I mean, there's great benefits to the economy because of the Fair Credit Reporting Act and the free flow of information, but the uses--what makes it work obviously is that all credit related information is, you know, fed into the system and then it's tightly controlled on the back end in terms of what's permissible in terms of the purposes for which it can be used.

So I just highlight those. We can go into that a little bit more.

But we also believe that multilateral and private sector initiatives have an important role to play in encouraging the development and use of privacy enhancing technologies and in promoting business and consumer education. So we've worked, you know, besides our bilateral work, you know, with India and also with China. We're actively engaged multilaterally with the OECD, the Organisation of Economic Cooperation and Development, in Europe; APEC, Asia-Pacific Economic Council, and through other groups like the Global Business Dialogue on E-commerce, the Transatlantic Business Dialogue, and the Transatlantic Consumer Dialogue.

So, as I said, despite the benefits of information sharing to the economy, the Department recognizes that U.S. business and consumer concerns about data privacy and

security, such as identity theft and industrial espionage, data sabotage, data mining--those are all real and legitimate. Those problems not only injure U.S. consumers and companies, but also hinder the growth of e-commerce and the development of trust in the on line environment.

A lot of these problems, though, are--they're transnational in nature and can represent a threat to potential victims regardless of where the bad actor resides or is located. So for these reasons, we believe that moves to bolster online and offline privacy--I mean on and off, both--and to safeguard business and consumer interests at home and abroad that those will--that will fuel trust and the broader growth of cross-border trade, online communications, innovation, technology and business.

MS. BRAINARD: Terrific. Thank you very much. And I think we'll come back and maybe drill down on some of those points. But let me bring in Kiran Karnik, who is visiting this month I guess from India, who is the president of NASCOM, which is probably the biggest and best known Indian IT services trade association. And he's in town during this time partly meeting with regulators, members of the Administration to talk about the Indian frameworks and how they connect up with the U.S. legal and regulatory frameworks.

Prior to joining NASCOM--I hadn't read your background before, but you have a great career--he was managing director at Discovery Networks and worked with both Discovery Channel and Animal Planet and worked for over 20 years in the Indian Space Research Organization, and I guess you're originally a physicist; is that right?

MS. KARNIK: Yes.

MS. BRAINARD: What would be terrific is if you could give us a little sense of what the Indian industry is doing. What the parliament and the Indian government is doing right now, recognizing that India has this growing stake in the offshoring of IT-enabled services and that any breach of privacy or security could really lead to a big backlash.

MS. KARNIK: Absolutely. Thank you, Lael. And I want to thank Brookings for this opportunity to share a few thoughts from what we are doing in India, and to share them with our distinguished panelists here and the folks here with whom we can have a little session on in interactions and suggestions as we go forward.

What you asked for is exactly what I thought I would I start with is to give you some sense of what is happening in India and what we are trying to do.

But before that, let me back off for just a moment and say--I think Dan set the stage very, very well. I want to say that from all points of view, this whole aspect of making sure that there is first confidence in being able to move, transfer data and to e-commerce is critical, because that's the business on which we survive. We thrive.

Second, the fact that the data is moving far away very naturally gives rise to concern. I mean we can all say that distance doesn't matter any longer, which is true, and we all know it, and yet deep down somehow, for most of us from most of these generations, something that's far away, you always worry a little bit whether it's a physical person with whom you're close with who's gone away to a far off country or whether it's your data going somewhere else.

So we very much appreciate the concern, but the fact that the data is now residing somewhere in a distant land, somewhere far from where you are is bound to give rise to more concern than if it's sitting next door to you irrespective of the fact about whether it is, you know, in any more danger here than here. So one appreciates that point.

And third, the fact that Lael just mentioned we're acutely conscious that because of these two factors should there be any problems, they are going to be seen in some sense in a harsher light than what might happen if they were equal than breaches in the U.S. It's sort of odd in any other customer country with whom we work--in the U.K. or Europe. And that's the overarching kind of background within which we've tried to look at what is it that we need to do.

That clearly, you know, indicates that what we need to do is to make sure that not only is there confidence with regard to the legal framework, but that there is comfort on the legal framework; comfort comes from the fact of saying there's some familiarity. It's something like what I know and which is same as here.

And second it comes from a confidence that should there be a problem, action will be prompt, severe, and immediate. And I think that's important from a deterrent point of view. And that's the sort of factors we have kept in mind as we have worked on this.

We do have very strong privacy provisions in our constitution, which was framed in 1950, long before any of us thought of e-commerce or movement of data. These provisions stem from the sort of international things that are existing, many in the U.K., but to some extent in the U.S.

And so the right to privacy is enshrined in our constitution as one of the basic things, and that is what the legal fraternity has been using in the past, long before other things came up in terms of any infringement of individual privacy in any form.

That's been topped up very specifically in the area information technology and e-commerce by the Information Technology Act, which was brought into place in the year 2000, four or five years ago, which broadens and specifically lays down things with regard to privacy for electronic data, the data movement, devices in which it's stored--the whole host of things which would be of concern in today's world of electronic data movement and electronic commerce.

And between these two, from all the feedback we've had in checking with lawyers in India and around the world, the system is robust and good.

However, in reexamining where we were--a process which we started about a year, a year and half back--we saw that the kinds of laws that exist in Europe and to some extent

in the U.S. are sometimes a little different, sometimes a little tighter. So we went and revisited this whole legal framework that we had in place, and we found that the--you know, the most stringent one one could possibly look at was the European Union one. And the first reaction was saying let's just follow that. We want our framework to be strong, and we want to prove it strong. So let's take the European framework and apply as it is to India.

But we soon found that the European framework as it exists, if put literally into place, is frankly very inhibitory of any kind of business, because it in some sense stalls the very movement of data. It's going to make life very difficult for anybody doing business in this area. It was drafted, you know, 10 years ago and has evolved, but clearly it was drafted in a different era, when you didn't have net and web access, when data moved from one point to the other, and so there are a different set of concentrations.

So what we did was look at the U.S. law, and to cut a long story short, what we have gone about is the process of know trying to see how do we bring about some degree of harmonization between what exists in the U.S. and what exists in the Indian statute books so that the point Lael was making earlier, recognizing that this is an international issue where, as Dan said, many of the things are [inaudible] extraterritorial. Since extraterritorial sovereignty is a problem, can we make the two laws so similar so that it doesn't matter where the crime is committed or where the person is the law applied is almost the same. That's the kind of thing we've worked with.

We worked very closely with a U.S. law firm which did a gap analysis to see what are the differences, and then has come out with suggestions. We then worked with Indian law firms to try and see how this will fit into the Indian framework to make sure it's compatible with all the other laws on the statute books in India and what changes need to be made in those.

And we've now put together a set of amendments which are being shared with many in the community here, including our customers, various chambers of commerce, our friends in the ITA, folks in the Administration. And the feedback we have is very, very good. It seems okay. We are taking into account of a few more suggestions, and this will be in place--we expect the final enactment to be done around the end of this year, plus or minus a few months in the legislative process. But we would have them all together in place and moving into the legislative pipeline in about a month to a month and a half. That's on the legal framework, and I spent some time on that because I think that's a point of some concern about where the legal overall framework is.

But from our point of view, there are a couple of other things which I want to touch on very briefly, which are as--and I would argue sometimes more--critical.

The first is enforcement, because you might have very tight laws. If enforcement is poor, it doesn't mean anything. On the other hand, if you have laws that are, you know, reasonable, but not too tight, but you enforce them very stringently, that itself has a salutary effect.

So we worked very hard in making sure the enforcement is appropriate, and from industry we have taken an initiative to help to train a very large number of police officials. We have helped to set up a cyber crime lab, which is the sort of forensics of cyber crime to track cyber crimes and get down the evidence, nail it down, put it in a form which you can take to the judiciary and actually get a conviction.

So we've worked closely with the enforcement agencies on everything from awareness and education to actually helping to provide training for them to be able to get these into place.

We've also done some amount of awareness building with the judiciary, because after you do all this and the judge says, yeah, you know, you've committed a crime, but, you know, pay a hundred dollars and go away. You don't want that happening. So we've taken two safeguards on that.

First, the law itself lays down certain minimum penalties, including jail sentences. And we've educated the judiciary about what the seriousness and the impact of these crimes to make sure that they take them as very serious crimes. In fact, some of them in the legal parlance have already been defined as criminal offenses, so it's fairly strong there in that.

Finally, the last part of this which I think is, as I said, as important if not more is the recognition that what you need to do is to see to what extent can you preempt this, to what extent can you build in factors which prevent this from happening and track it down immediately and instantly, and that means looking inside, because much of this sort of crime emanates from inside the company, inside the people who have authorized access to that data in their day-to-day work.

So we've tried to put into place a whole set of best practices, taken from around the world. Indian companies are good at it. We've picked up from elsewhere, and put them across the whole industry. And these include from the very simple obvious ones, which most of Indian companies already do like access control only permitted people in on a need to know basis, biometric entry, electronic firewalls, no pen, pencil, paper, floppy disk, not even a cell phone, because even if the cell phone is off you can take a picture with a camera phone and download the, you know, the screen can be dumped onto that. So none of those. So those restrictions and you know constraints are there.

But beyond that we are now working on something else which I think would be a major contribution. We are working on an employee data base which will help to get the

background data and background checks of individual employees. We're acutely conscious that just as we talk of privacy, there's a privacy and individual rights element to our employees, so I want to stress that we are not going overboard on that. All we're doing is collecting known data which is part of what they put out in their c.v., making sure it's verified by a third party, and then putting it all in. And that data will be owned by the employee. So the employee owns that data base.

However, an employer may ask for that access to that data base to ensure that all the background checks are in place and have been done. So if you go for employment, yes, the employer is going to ask you, and it's being checked out. And if not, it will be difficult.

So very frankly de facto, in reality it's going to be that this data base is going to be critical for employment here because the background checks today are, for good or for bad, increasingly necessary. So that's what we're putting in.

And the final part of this within industry is to put in place a self-regulatory organization. We are in the final stages of putting together the ambit and the framework of that, and this will be backed up by the law. So you have an internal policing system within the industry, backed by a legal framework which enforces that.

Between putting all these together, we are very confident that you will have a very, very strong system that first tries to, you know, minimize any kind of offense, but I will use the word minimize very advisedly. Frankly, and, you know, many people in industry don't like my saying so, but the fact is you can't have a hundred percent foolproof system. And so you try to minimize any such thing and make sure that the same one is plugged and doesn't happen again. But far importantly, if there is any breach, you should be able to capture that immediately, identify the individual, prosecute the person, and take immediate action, because

the deterrent effect of that, in turn, is very strong, and so you get a reducing number of possible breaches.

That's the strategy at least as I see going forward, because I don't think, try as you might, you're going to have a hundred percent foolproof system, which is why you need that legal enforcement framework. You need the enforcement agencies to act promptly and efficiently. You need to have them educated and aware. And that's, therefore, the total cycle in which we are working.

Given these as we've put them together, I'm confident that as we've had in the past in India, we will have a very, very strong awareness and a strong actual implementation of data security, cyber security and privacy. An occasional breach one can't rule it out, but when it does happen, we're making sure that the action is immediate, prompt, and, as I said, severe. And that severe action is laid down in the law and further, you know, and then further amplified by the fact that the judiciary knows about the seriousness of this.

I just--sorry I've taken longer than I wanted. I just wanted to share this totality of the framework, and I'll be happy to answer more questions on it as we go further.

MS. BRAINARD: Terrific. Thank you. Let me now get a voice that I think is more focused on the consumer concerns and ask Evan Hendricks to enter the debate.

Evan Hendricks is a long-time editor and publisher of Privacy Times, which reports on privacy and information law, including FCRA. He also has been and I guess currently is also a consultant on privacy, both in the past for the U.S. Postal Service and now the U.S. Social Security Administration.

And, Evan, I guess I wanted to start by just asking you to give a sense of the frameworks that Dan and Kiran have described, where do you see holes? Where are there concerns, and in particular where are the holes different because the data is moving past the

waters edge, as oppose to the concerns that we already have within the domestic market, what is particularly concerning or missing when that data gets transmitted to overseas environments?

MR. HENDRICKS: Well, I mean that's an important question, but you really have to understand the fundamental domestic base here. When information is outsourced--and I think you made the point that sometimes the greatest threat to security of data, and, therefore people's privacy is when people on the inside have authorized access to the information, and they use it for unauthorized purposes. And some of the greatest breaches have come either from conning the people on the inside or from bribing people on the inside. And since outsourcing is about chasing cheap labor, you're lowering the cost of bribing. So that's an immediate concern to the security of the data.

But the fundamental issue for Americans right now is that we have holes all throughout our system, which I'll discuss, which means that as information goes overseas, it starts blurring the line over who is responsible for it--the chain of custody over that information.

And I've already seen cases where personal information of Americans is outsourced in a routine way, and that the information is becoming again--the accountability starts degrading beyond the weak privacy laws we already have in place.

I wanted to thank Brookings for the opportunity to talk here, because the two areas that I've seen Brookings do work in privacy is a good place to show--to illustrate--what are the problems in our system. In fact, when they asked me to come talk, I was going oh, oh, Brookings is doing privacy again.

One of the times was the before Dan mentioned the Fair Credit Reporting Act. That is our best privacy law. It's our most comprehensive one. It gives people right of access to their data. Right of correction. It incorporates all of the eight principles of the OECD guidelines from 1980, which is the gold standard of privacy. So you have private right of enforcement.

You have security standards. But industry was very worried because in 2003, there were seven provisions of that federal statute that preempted state law. And those provisions dealt with very big money issues, like the pre-approved credit card offers you got or on the sharing of affiliate information among huge conglomerates. Like Citibank has about 1,500 affiliates, and they have a good revenue stream by sharing information among their affiliates.

Industry was worried that if the federal law--if the preemption expired, states would start enacting protections in those areas. And so there was research done in this area. Brookings put out a report, with the AEI, by the way--this is a joint AEI project--which said that basically there are no problems for consumers. This law is working well, and we should simply extend preemption and make everything permanent.

That's not the way it went. Congress did make preemption permanent, but they also spent the whole year overhauling the law and making strong consumer protections.

The other Brookings effort was done by Bob Litan and Peter Swire, which was looking at the European directive, and this is another time where industry was very concerned because the European Directive wants to ensure that information on Europeans doesn't go to countries that have inadequate privacy law. And so they look at privacy as a fundamental human right, and our industry was looking at this as an impediment to trade. And the Europeans said no. We're just trying to protect the information on our citizens, and that's--we have to do it in a global economy. And the Litan and Swire effort was basically attacking the European Directive from the industry point of view.

So then I said well this is the third time they're looking at, so maybe the third time will be the charm. Brookings, along with these efforts and industry, has always looked at privacy as an impediment to organizational prerogative. And the reason privacy is such a

powerful issue is that we all care about our privacy, and individuals look at the information like this about me. This should be my information. But that's not true under American law.

Under American law, if they collect your name, they own it. And that's why in the recent Fair Credit Reporting Act debate, Congress struck a balance. They didn't change the fundamental ownership issue, but they said that you have a right to a free credit report.

Now, keep in mind that people think of privacy as something about hiding data or secrecy. Privacy isn't secrecy. Privacy is informational self-determination. It's preserving the individual's right to have reasonable control of then information. And from a societal point of view, the purpose of privacy is actually to have the free flow of information.

The reason that the Europeans adopted this Directive is because they had all these countries in Europe, and they wanted to make sure there could be free flow of information to help facilitate commerce and all sorts of other organizational prerogatives. But they knew they couldn't make that happen unless they had privacy guaranteed in law, with enforcement. So the purpose is that you have the Directive is to and create the free flow. And that's what we would want in this system with outsourcing. We want obviously--outsourcing is happening and it's going to continue to happen. It's going to continue to increase because it's part of history for capital chasing cheaper labor. And so the technology allows the information to go to places like India, but we should also remember that India is responding to this issue. There's also outsourcing to countries like the Philippines, Jamaica, which is where Equifax, the large credit bureau outsources our credit report to for dispute handling. And I don't see those countries really responding the same way India is here.

But the--I think that you have to--in terms of understanding the holes in the U.S. system you just have to look at this latest example of Choice Point, and I don't know if everyone saw the story. But Choice Point is a huge data base company. It was a spin off of Equifax. And

what they do is they pull together all the publicly available records for employment background checks to sell to the government, and they basically--it's a claim that they have 19 billion records--drivers' license, home ownership. And what happened is what appeared to be a Nigerian fraud ring, which seemed to be the most expert in this area, posed as businesses and up to 50 dummy businesses so they would be able to get into Choice Point system and have the run of the place, and the end result was that a 145,000 people, individuals, got letters saying that their information had been compromised, and at last count there was at least 750 victims of identity theft, because they were doing it for the purpose of committing identity theft.

And so this put a spotlight on Choice Point. I wrote an article in the first Sunday of the Washington Post Outlook Section about this.

First of all, the only law in terms of that requires that people be notified when there's a breach of their data is in California. So the first came--announcement of this came out when a Californian got a letter and Choice Point said they are going to be sending letters to 35,000 people who are in California because that's what was required by law. Well, that afternoon the questions started flying into Choice Point from me and a lot of other people saying why aren't you going to notify the other people in the other parts of the country? And their only answer could be well, it's not required by law. So they changed their tune and they decided that they would send the letter to other people. And that's why 145,000 people got notified. And that's why in privacy, when you're talking international sphere, privacy is a race to the top.

That's why India, in dealing with this issue, cannot simply adopt the U.S. standards because not even Americans will be satisfied with that. I mean Americans will say no. Our information is going, and it's only protected as well as U.S. law? That's not going to be good enough. And clearly, if you can take the best from the European model and the best from

the American model, you will have a better system of protection than either Europe or the United States.

And so, and I think as you talked about the legal system, I think you have to go a step farther and that's the organizational culture that is implementing privacy. One parallel is that we have one of the best laws in the world, the Freedom of Information Act. It gives us the right to get information from our government, and if they don't give it, we can sue them and force them to give it, and they have to pay our attorneys fees.

But this is a law that it has like a 20-day time limit and that's seldom implemented by these agencies. A few do it, but most of the time it can take months or even years to get information you're entitled to get in 20 days. So it's a great law, but the organizational culture is not there to really implement it successfully.

So that's why this is a very three-dimensional and deep issue and why it requires the combination of law. It requires good organizational practice, and it requires the good use of technology.

And I'll close with just this one example. The credit reporting agencies now have services, which they're selling for about $100 a year, which means you can get online--regular online access to your credit report and be notified if there's a change in your credit report, which is really terrific because that means if some--you live here, and some car dealership in Texas pulls your credit report, you get that notice and you know that you weren't in a car dealership in Texas and that becomes a great way of warning you about identity theft.

The point is that this is a system where individuals--the technology is there, the market is there--individuals are as plugged into their own personal information as all the institutions that are out there trafficking in it. And so that is basically the model where we need

to go so you basically have individuals monitoring their own information and alerted when there's significant changes in it. Thank you.

MS. BRAINARD: Thank you. Now, what I'd like to do is get the last voice in, which is from industry. And let me just introduce our speaker. Jeff Lande is a senior vice president with the Information Technology Association of America, and heads both its IT Services and Software Business Units, and I think is the Chief Expert on Privacy as well within the organization. ITAA, for those of you who are not familiar with it, is the oldest and largest IT trade association in the country, and accounting for over 90 percent of all the IT goods and services produced in the United States.

Jeff, as--it would be interesting to get industry's perspective on this, whether there's a lot of initiatives underway now in different parts of industry to try to deal with these issues preemptively. But also if you could talk a little bit about some of the things that are being proposed or pending either at the federal level or at the state level, and how industry views them--things like opt in provisions or opt out provisions. Some of the informational requirements, potential right to know requirements, that are being discussed. And also if you would a little bit reflect on the difference between the European and the U.S. framework and whether something in between, as Evan is suggesting, would actually be the best of all worlds kind of a framework.

MR. LANDE: Right. Well, thank you, Lael, and I'd like to thank Brookings for hosting this important session. Again, today, it's always a pleasure to appear with Karin and Dan on this. It's also always fund to hear Nick speak. He keeps us honest. He always pushes things so far to the extreme as when we shut down commerce. So it's interesting to have someone like that there, too.

Nick did say that much of this is just about--I'm sorry.

MS. BRAINARD: Evan. Evan.

MR. LANDE: Just about the chase for cheap labor, which isn't true. There's been a labor shortage. There's been a skill shortage in the States for years. Much of this is about the chase for the best and the brightest worldwide. And also U.S. corporations, when you look at the Fortune 500, generate the bulk of their revenues off shore, so it's also about setting up operations where you can service your clients.

Now that being said, U.S. industry does clearly understand that this is a shared responsibility. You know, privacy is a major concern. Consumer privacy is something that affects everybody. It's something we're all concerned about. Consumers have a role to play in this. Law enforcement has a role to play in this. The retailers, the banks, health care providers, the IT vendors, law enforcement, the judiciary--everyone has a role to play in this.

Some of the things that the IT vendors do and they're constantly vigilant on this: physical security and cyber security. Physical security: the background checks, making sure employees don't have access to take data out--the types of protections that Karin was mentioning.

Cyber security: constantly monitoring data flow; constantly monitoring access of data; walling off on certain things; encryption.

Now, much of this panel I thought was really going to be about privacy in the era of global sourcing, global trade. But that's something I haven't heard. I've really heard it framed from the standpoint of the U.S. versus the rest of the world with the base presumption being that things are worse once the data does travel great distances. I'd argue that consumer protection, consumer privacy is something that we have to be concerned about everyplace, and there's really no difference between the States and overseas; and that there are very strong protections in the States right now, whether it's Gramm-Leach Bliley, whether it's HPA, whether it's FCRA, whether it's COPPA--all of those are very strong protections, and the enforcement mechanism is what's key in this.

And I think that much of that is also mirrored by the fact that we've had dozens of measures come up in the States this year focusing on this. We literally have hundreds of bills in 42 states last year that came up that touched on global sourcing, that touched on privacy. Not a single one of those were enacted. And that's not just because industry has great lobbyists. It's because at the end of the day there was a recognition that the current statues are sufficient.

There are a couple of provisions floating around in Congress right now; on by Senator Clinton. Those likely will not go anyplace because they draw distinctions between data that will be transferred inside the States and cross-border transfers that aren't official and that will cause difficulties in terms of trade agreements overseas and will ultimately hurt consumers and consumers' choice.

So just bringing that back, I'd say that this is a red herring, looking at this issue from the standpoint of the global framework. The U.S. laws do carry over to the providers overseas. Under HPA, under Gramm-Leach Bliley, there are requirements that the U.S. vendors, the financial institutions, the health care providers have contractual arrangements that bind their offshore vendors to the same protections that they have in the States, and that also the real emphasis should be on law enforcement and also ensuring that the types of breaches that have occurred due or to human errors and a failure to follow internal corporate procedures are taken care of. For example, in the Choice Point instance, what really happened there was that they didn't go in and check the authenticity of these businesses requiring the data. Choice Point does have policies requiring their employees to do that. They didn't do that. There was a breach at Northwestern recently where a laptop was stolen with records of alumni. That kind of thing shouldn't happen. During the first Gulf War, if memory serves me correct, one of the military attaches in the U.K. was carrying a laptop with strategic documents on there. He went in for coffee. His car was broken into and the laptop was stolen.

Those are the types of human instances that shouldn't happen.

MS. BRAINARD: Well, let me do the following. Let me ask if there are some questions from the audience and let's bring in the audience, and I'll hold off on my own question. Yes? And if you wouldn't mind identifying yourself and your organization. Thank you. We have a microphone in the back.

MR. BOURILIO: My name is Rami Bourilio [ph.], and I am the commercial counselor at the Philippine Embassy in Washington, D.C. I just want to make a short comment on a statement that I heard to say that a country like the Philippines does nothing of the sort of things that India does in order to promote data security and privacy among its service providers, our country being one of those who have recently entered into the global outsourcing market.

My comment here would be that the direction we're taking in this issue is basically the same as what India is doing. In terms of constitutional provisions for privacy, there exist those in our constitution. We have an e-commerce law that does have provisions on data security.

The only place where we could say that India is ahead of us is in fine tuning this basic legislation to sort of approximate more fully what exists in the United States. We have taken a look at the EU regulation on data security. We have examined the safe harbor agreement that the United States has with the European Union, and we are aware of the intention of law, such as those proposed by Senator Clinton in order to bring about data security. These are being examined, and there is a full intention to adopt legislation that will approximate that.

But you must remember that India has a 10-year lead time. It's advanced by 10 years in compared to the Philippines. Our outsourcing industry has really just taken off in the last three to four years. But these are being addressed.

One of the most recent measures we have taken in order to update the service providers on precisely this issue was to invite the president of ITAA to the Philippines last--I think it as last February--to speak before our service providers on precisely this issue. We also have in that seminar the vice president of NASCOM, because, as we said, we are, of course, guided by what India is doing on this matter.

So these are the things that we have done. And we intend to continue doing this. I'm also happy to hear what the representative of ITAA said that while this process is taking place, it doesn't mean that American standards are not enforced on the Philippine service providers because, as was mentioned, these are fully enforced by contractual arrangements that require that the same levels of security be adopted by the service providers in addition to certain physical measures or technological measures that have to be taken in their premises to enhance the security. Thank you.

MS. BRAINARD: Thank you very much. Let me just ask Evan to comment, not on the Philippines in particular, and I'm glad that we got another voice from some of the countries with whom we're doing so much offshoring, but I wanted you to comment on this issue of whether, in fact, the contractual or subcontracting obligations, for instance, of a financial institution under Gramm-Leach Bliley are seen as satisfactory that the company really has full liability for managing that supply chain or whether there are concerns that the law doesn't go far enough there.

MR. HENDRICKS: Yeah. That's why I spent a lot of time talking about what is the domestic situation. So if you're Gramm-Leach Bliley make as requirements that banks have security in place. It requires that they do something as opposed to nothing, but it's a general standard. The problem is individuals don't have a right to enforce their rights under Gramm-Leach Bliley. So if you're contracting to India or the Philippines or Jamaica, and there is a

security breach and you're upset or damaged by that, you basically don't have a remedy. So it's a law without a remedy. Gramm-Leach Bliley is only a glass that's either half full or half empty, because, for instance, under Gramm-Leach--it doesn't implement the full fair information practices of the right of access to your records. I mean huge banks like Citibank or huge organizations like Choice Point can also have detailed files on you like a credit report, and you don't even have right to see what information they have. If there's a security breach, you don't have a right to--

[TAPE FLIP.]

MR. HENDRICKS: --to notify you of it. And if you become a victim of identity theft, and they were grossly negligent, you don' have a right to recover a remedy from them. So that's the problem. It's like if you're just contracting to conform with, you know, weak American laws, then privacy is not adequately protected, and so that's the foundation that needs to be worked on there.

MS. BRAINARD: I don't know whether Dan or Jeff just wanted to comment on that in terms of adequacy of that framework?

MR. CAPRIO: Well, I mean, Evan is speaking to the--I mean both to Gramm-Leach Bliley and to the Fair Credit Reporting Act, and I mean I commend the article to you that Evan wrote in the Washington Post a couple of weeks ago, in the Outlook Section, was I thought a very fair and balanced perspective. What's important to sort of keep in mind about Fair Credit Reporting Act was as we're discussing the extension of the preemption of the seven provisions that were expiring, the elements that sort of came along on top of that in terms of some criminal enhancements for identity theft, but the biggest one of all is, you know, the availability of a free credit report, which, you know, were phasing in the entire country. The West Coast is already phased in. I think the Midwest is phased in. And by September 1st, the entire country will be

phased in. I mean in Virginia and Maryland I think we're in that last chunk. You know, we had to bring the country online in four different pieces.

So what we're seeing, though, because of that is, as I said, the criminal enhancements in the statute that--and it played out in Choice Point that, you know, if you're engaged in criminal identity theft, you're going to do jail time. So the, you know, some of the Nigerian ring was convicted under California law and I believe also sentenced under federal law, if I'm not mistaken.

But the other part is that the availability of the free credit report and so that, you know, if monitoring your credit report is always something that we've recommended. When the entire country comes online that will be much, much easier, and that does afford, you know, a much higher level of protection. And, you know, many of the credit card companies I believe--some will make you hold, you know, at zero; others it's 50--you know, $50 is the maximum, so, those are all important provisions and important protections along the way.

MS. BRAINARD: Okay. There was a question over here.

MR. : [Inaudible.]

MS. BRAINARD: Okay.

MR. HENDRICKS: I'm sorry, but one thing that's interesting on top of what Dan said to see is you do have some companies now beginning to look at this as a differentiator. So market forces are coming in. A couple of insurance companies and a couple of financial institutions are saying if you're a client of ours and you're a victim of identity theft, we're going to come in and we're going to support you fully. And we can provide you with all these services to try to rectify that. So that's another thing that's moving along.

And I just wanted to say one thing to follow up to the comment from the gentleman from the Philippines. It is great to see forces trying to harmonize these laws

throughout the world, but I'd also like to say that there's a global organization called WITSA, the World Information Technology and Services Alliance. NASCOM is a member. ITA is a member. Our president Harris Miller is the president of WITSA.

It's a global consortium that picks up 64 nations, and has the leading IT associations from each; and there is a very strong movement inside WITSA right now to have all 64 of those IT associations working together to address this problem and then going back and then dealing with their own governments and encouraging action. You know, I think ITA and NASCOM are working very closely with the Department of Commerce and the Indian authorities on their act. We work closely with the governments and the associations in all of the major IT centers throughout the world to hopefully address this problem in the short term and long term.

MS. BRAINARD: Yeah. A question. Okay.

MR. : Using the microphone?

MS. BRAINARD: Yeah. There's a mike right back here.

MR. SCHROEDER: Thank you. Hi. I'm Robert Schroeder with International Investor, and I'm going to ask some very specific questions, just because we always believe the proof is in the pudding, as they say.

I'll be very brief. I promise.

First of all for Mr. Karnik, you pointed out a lot of effort is going into the legal system there, and enforcement is something that you believe in as well. India has been in this business a couple of decades really now. Can you give us any--and I'll wait for the answer after I'm done--can you give us any indication of the numbers of enforcement actions, indictments, number of institutions that have been held responsible and fined in any way?

For the gentleman, Jeff, from the TAA, I would ask you--you mentioned background checks of employees. Even in the U.S., domestically could you provide us reasonable numbers, estimates, of the number of background checks on employees here? How many red flags have come up? How many employees have been excluded from joining an organization as a result of those, and whether or not this extends beyond the U.S.? Are we requiring background checks of all IT employees in 200 countries around the world?

Number three, Department of Commerce long recognized one of the mandates, of course, to export not only goods overseas but that the IT industry being an important part of our commerce, are there any provisions, restrictions, guidelines, since the U.S. is the most important market in the world still for countries trying to bring their goods here, for--to prevent or again guide companies who wish to sell privacy information, whether it be a Choice Point or whether it be individual exporters about their customers to those organizations overseas who are trying to export here?

I'm sorry, Evan, I don't have one for you.

MR. HENDRICKS: Don't ask.

MS. BRAINARD: All right. Well, let's take them in that order.

MS. KARNIK: You want me to go? Okay. But very briefly. You know, we've had a very, very few cases where--which have really come up, which is good news in terms of numbers that have come up. A recent one I can think of, a very recent one, where a fraud was detected. It was detected within a few days of its happening, about 10 days. The police investigated it, and a month the notice was issued and folks have been arrested already.

The court process in India is sometimes elongated. We are all aware of that. We are trying to accelerate it by special IPR courts, but the arrests and the action have been prompt.

However, having said that, let me add one more thing, which, you know, many of you will be aware of. In a country like India very frankly, it's as important as the conviction is the charges and the starting of the process because that person, somewhat sadly but not so sadly, is not going to get a job again. And in India, that can be more of a punishment than even going to jail because I mean putting it half facetiously in jail you get fed. If you don't have a job, you don't have social security nets in India which are as good as the U.S. You're going to starve. So, you know, it's a very, very strong deterrent to lose your job, which is sometimes as strong than the possibility that you might get convicted two years down the road. And I think that's worked very strongly so far in India.

I want to add something, particularly since you didn't ask anything to Evan, I want to take issue on him on something which relates to this, and I know it was an unintentional one. You know, this common perception--I think Jeff answered the basic thought of it that work doesn't move any longer because it's necessarily cheaper. It moves where there's talent and the best and brightest for the kind of work that you're doing. But this impression that because you are poor, you can be bought I want to take issue on that very publicly. I know you didn't mean that, but I do want to put on the floor, because now and again we get this little thing: you know that they're paid less; therefore, they can be bribed easily and corrupted. I think it's nonsense. Greed exists more at higher levels than at lower levels. Those who are poor have a standing and values of their own. So I want to debunk this even thought that because people are underpaid, therefore, I can bribe them easily. Nonsense. Let's get that out of our way.

The last comment I want to make again in relation to the enforcement one and I think that point was very well made by Evan I think in the Philippines comment. I'm very happy to see that there is, in fact, as Evan put it very well, a race to the top, because as different countries look at legislation and this is something we've done in India ourselves, that while we

have tried to harmonize very strongly with U.S. laws, we've also picked from places like Australia which have something which are additional and different and nicer. So you are getting a best practices emerging. And I'm sure as the Philippines does this as well, as David picked from what we are doing and takes it even higher.

So internationally for all us, each one of us, whose data may be residing anywhere in the world tomorrow, this gives a sense of great comfort, and I think we've got to work on it together. Besides the great [inaudible]. We work with others on this, so I think that's what I mean.

MS. BRAINARD: Can you just on this Australia point, can you give us a little more information on what is it about the Australian framework that is actually better than the U.S. framework?

MS. KARNIK: Well, if you permit my expert here, my colleague, Suni Mehta, is the one who's done all the work on that, and you want to say something, Suni, on what particular aspects of the Australian one?

MR. MEHTA: [Inaudible.]

MS. KARNIK: The definition of computer-related offenses. You know this is something else we have seen in many ways, and we have taken that ourselves. I'm sure others will take it further. Much of the definitions earlier related to a computer. Today, your data can be residing on your cell phone. It can be on a whole host of other devices. So these definitional ones in which lawyers make all their money arguing cases--they make their money in many ways, but this is one of the--I think we are trying to make sure that the definition of these terms like, you know, what is data, what is a computer, where is data stored are broadened to the point where it takes care of not today's technology, but technology as it may emerge later.

MS. BRAINARD: All right. Thank you. Jeff, background checks, red flags?

MR. LANDE: Background checks. That's a great question. It's also, you know, the impossible question to answer because, as you know, in the States, we're dealing with private corporations that are going through this. We're also dealing with private corporations that do these types of operations. So I can say millions of background checks are done annually. There are undoubtedly some red flags, but there's no way to put hard numbers to that. What I can say is most of the regulated institutions in the States that chose to outsource and chose to offshore, particularly in the financial services sector, what they've moved to do is require that their vendors conduct thorough background checks on all staff who work on this.

What they also require--as far as I know all the major financial institutions--require their IT contractors to do this: is wall off the separate dedicated facility just for their projects. So Citi, Morgan Stanley, Wachovia and such when they outsource, there's a separate office of the IT vendor just to work on those projects and that those people have to go through a certain level of checks that have been negotiated between the client and the vendor before they can touch that data.

MS. BRAINARD: And, Dan, your question to you.

MR. CAPRIO: Yeah. Thank you for you the question. I think the advice--if that's what you're asking--the advice is actually the same, you know, whether it's a U.S. company or a company that would be exporting or importing. And that is, I mean, you sort of start--I start from the fundamental premise that you can't have privacy without security. I think Evan mentioned or began to sort of touch on it--but the idea of creating a culture of privacy and security, and that, you know, if you're a company that's got to be, you know, embedded within the culture, within the company at the CEO level, you know, as a corporate priority. And, you know what that really entails and then this has been articulated by the OECD and the security guidelines, but what that's really about is awareness, accountability, and taking action.

I mean, as Jeff said, making privacy and security a part of your corporate culture and then differentiating, you know, as to your competition, on, you know, like Evan's terms, on sort of the race to the top.

But we believe that--I mean as a set of principles that a market-oriented approach is the preferable way to go. So that the way that I think of it really is in terms of four principles.

One is, you know, protecting privacy and security, particularly in working with government, but the need for a strong public-private partnership.

The second part, which we've all touched on today, but it's the need for effective law enforcement, both in the civil and criminal side. That's what makes our system work so well here in the United States.

The third component is that, you know, the promotion of education and awareness, you know, both within the company and of consumers and home users.

And then the fourth part, which is really what we strive to do at the Department of Commerce, which is to create and encourage that market for innovation and growth that allows the technology to be able to, you know, to be able to keep up or to be able to meet the needs. We talk a lot about, you know, baking privacy and security in, and fundamentally those are the kinds of things that market for innovation and technology, you know, can create--you know, the market-oriented or the private sector solutions.

MS. BRAINARD: Other questions. Yes. A gentleman over here.

MR. BYRD: Hi. Good morning. John Byrd [ph.] with the MAPPS organization, Management Association for Private Photogrammetric Surveyors.

And basically I was hoping your distinguished panelists could comment maybe on Mr. Karnik's point of view of there not being a hundred percent safeguard for any kind of infraction. Going through when it comes to mapping and satellite imagery of the offshore

contracting of mapping and satellite imagery going off shore, and basically if you can touch on that, and the personal privacy concerns versus national security concerns, specifically on America's critical infrastructure data, like utilities, nuclear power plants, and so forth. If you can kind of touch on that if you can?

MS. BRAINARD: Anybody want to take that one on?

MS. KARNIK: Just a very brief comment. Your point is well taken. I didn't mean to exaggerate my point about hundred percent foolproofness [sic].

What I would say is that you make these systems as foolproof as you can, but at the end of the day, just as in the case of, say, disaster recovery, business continuity plans, you've got to have a contingency plan and contingency operation for what if kind of situations.

Now, in situations of national security, you take care of this by assuming that it was a breach it's yet controlled in your outer wall, so to say. You know, so you have multiple layers of security. So if there's--the first one is breached, we have something else that yet protects it, and that's the way traditionally, you know, national security things you do it.

But you do assume a breach, and as far as I know, you cannot but assume that somebody will get in there, and then you just contain it within its prevented from really moving outside to a danger zone.

That's the only way I would put it figuratively. But, yes, the effort to continue to make it foolproof is something that will go on and must go on. I don't want to minimize that, but simultaneously you need to look at what you need to do to make sure that the deterrence is so strong that these things don't take place. So it's going to be an ongoing one. It's like, you know, it's like missile and anti-missile to take the same analogy from the security area, which one knows is going to go on. There's no hundred percent foolproof missile protection system that you're ever going to have.

MR. HENDRICKS: And with regard to national security since you raise that, I'd make two points. One, just as with consumer privacy there are historically great threats from the inside as well as from the outside. So we need to be vigilant about both.

The other point I'd make is with regard to true cases with national security implications, there is a strong international framework that preserves the right of that government to keep all that work within its own borders and within the framework of just having citizens work on it. So that's really a separate entity than issues of consumer data and that type of thing.

MS. BRAINARD: There's another question right next to him.

MR. SCHMIDT: Yes. Ted Schmidt [ph.], National Academies of Science.

I had a question. Jeff, you mentioned at some point Choice Point had policies in place that had they been properly carried out, this may well have been prevented. That sort of goes to that baking in the culture issue.

Are those policies mandated legislatively? And, if not, could another Choice Point company set up and not have such policies in place? And if they are required, what sort of enforcement, since we've talked a lot about enforcement, what sort of enforcement is happening?

MR. LANDE: That's a very good question. With regard to Choice Point, from my understanding from talking to some of their folks, they do have the policies in place. They believe the corporate culture is there. However, there were some individuals who didn't execute on that policy.

You are right that there probably are companies out there that don't have those sorts of internal policies. I think that there is a race to establish those types of best practices and move in that fashion. Market forces are driving that, given the publicity around this. Given the consumer outrage around this, there's going to be a shift to work with those companies that have the strongest protections.

There is not government regulation as far as I know right now that cover those sorts of specific provisions, and I would say that the establishment of those types of protections would actually be harmful and would hurt both the enterprise and would hurt the consumers long term because it would prevent them from getting financing in a rapid fashion. It would prevent them from getting access to certain types of deals and such.

MR. HENDRICKS: Could I comment?

MS. BRAINARD: Evan, yes.

MR. HENDRICKS: Yeah, no. Choice Point had little in the way of policies in place. I can't believe that you think that they did. They came up before Congress, and the Senate Banking Committee had a hearing. The Vice President of Choice Point was there. They were asking Choice Point how much money do you spend on security. And he didn't know. Senators Schumer and Bunning were so upset that they said that Choice Point should get out of the business to be able to--after everything that happened here, like one of the worst breaches in history not to know.

The other thing Senator Bunning read this comment from a federal judge when Choice Point was sued under the Fair Credit Reporting Act. They couldn't get this woman's insurance report correct. They kept polluting it with bad data, which caused her to get denied for insurance. And this is the Chief Judge in the federal court in Kentucky. He says: "Choice Point never took responsibility for assuring that its data was accurate. Choice Point never really explained the computer glitches which apparently caused this problem. To this day, the Court is still unclear what procedures, if any, Choice Point uses to insure the accuracy of its mass circulated reports."

Now Senator Bunning read that passage to the Choice Point Vice President, and said, well what procedures do you have in place to insure the accuracy? And he couldn't answer.

And you can actually watch this on the--they still have the video up on the Senate Banking Committee web site.

I think the good news here is like if you want an example of how to do this right, and it goes to the issue of transparency. I think I recall seeing deposition testimony from one corporate officer saying that they instruct their operators not to admit that they're in a foreign country. I think every person has a right to know if your information is being outsourced, and that corporations should not lie to consumers about it. But unfortunately, I think that's going on and quite widespread.

But if you look at what e-Loan is doing, e-Loan is--Cris Larson, the CEO, is a fierce privacy advocate, and I think their standards of integrity are quite high. They basically say if you don't want your information outsourced for this come during regular business hours. But if you want the convenience of 24-hour service, that's--you know, in the after hours that we have to outsource information, but by being transparent about it, they give you choice. If this is important to you, you know, make sure you come, you know, during the schedule. And if you're not really worried about it and but it's more important that you do something late at night, then this is how we do it.

And that's the kind of transparency we need for people to make good choices in the market.

MR. CAPRIO: I'll just chime in here. I believe--it might have been the hearing that you're referring to, but there have been a couple hearings and there will be more hearings. But the Chairwoman of the Federal Trade Commission, Deborah Majoras, testified I think Senate Banking--Senate Financial Services and said that, you know, the problems around Choice Point really create an environment, you know, to look at some legislative remedies.

And one of the things that she pointed out was the need for, you know, a federal breach notification law that's workable in some fashion. Another issue that she pointed out was that--we've talked a lot about Gramm-Leach Bliley and the safeguards rule--but, you know, let's have a vigorous debate about whether or not--you know, because it's not clear that the Gramm-Leach Bliley safeguards rule, which applies to financial institutions, which in the FCC and the functional regulators just came out with some guidance, but it's not clear that the Federal Trade Commission, you know, has reached under the Gramm-Leach Bliley safeguards rule to reach into Choice Point. And so that's a debate and a dialogue that I think we need to have going forward, and that was, you know, part of her testimony, and so that's--you know, that's certainly a worthwhile and useful exercise. And that's what's so important about all of these issues in forum like this is that, you know, to have the dialogue when we have a problem that came up like a Choice Point.

MS. BRAINARD: Let me just--before I'm going to get the last few questions. Before I do that, let me just pick up on Evan's point about right-to-know and just ask Jeff and Kiran to comment.

There are a variety of proposals out there, and these are seen I think as the least intrusive, about providing either the people who are at the institutional level--the UC examples come to mind--or at the individual level--the right to know when their information is moving overseas. How is that viewed in the business community? How is that viewed by foreign providers?

MR. LANDE: Well, with regard to the right to know provisions as they've been drafted thus far, I'd say that the vast majority of them are very problematic, for example, with regard to the call center operations. Most of the provisions have come up at the state level, and there have been a significant number of them not only have called for the right to know, but they

would have also required the enterprise to reroute any of those calls back to the States if the customer objected to speaking to someone overseas, which would essentially require you to have duplicative staff in both operations, vastly increasing costs. So that we have a real problem with.

With regard to the other provisions, it would depend upon how their drafted. If it's drafted in such a way that industry and consumer privacy advocates can agree--and I do believe that there's common ground there--then I'm certain that we can live with it.

MS. BRAINARD: Kiran, did you have a comment on this one?

MS. KARNIK: No. I think Jeff's answered it. I go along with him completely. You know, I do want to stress again that in all such cases, tacking on to what he said, the contractual arrangements transfer the same kind of requirement to any work that's offshored outside. So whatever needs to be done here will be done there.

But, as Jeff pointed out, some of these create practical problems, and I'm sure they can be resolved in terms of the intent of what is to be done if people on the two sides--

MR. HENDRICKS: Well, Jeff, how about the principle? Should corporations continue to be allowed to lie to consumers about outsourcing? Again, do we have agreement on that principle?

MS. BRAINARD: What do you mean, Evan?

MR. HENDRICKS: Huh?

MS. BRAINARD: Could you be a little bit more specific?

MR. HENDRICKS: Well, I've seen cases where it's policy to not admit to a consumer who's asking that the information-that their information is being outsourced. So basically they're lying to consumers about outsourcing. Do you think that that should be allowed to continue or do you think corporations should have to tell the truth about that?

MR. LANDE: I would say--I mean the instances that I've been in, where I've actually asked where I'm speaking to someone, where it's been offshore those companies have just said I can't tell you that. If I as a private individual was lied to, I would have a problem with that. I do not believe that corporations should, as a practice, lie to consumers. If they chose to say, we can't tell disclose that information, then the consumer can form any assumptions that he or she wants and take action accordingly, which is an appropriate action for both the consumer and the corporation.

But I agree with you that a corporation should not as a rule of thumb lie to its customers.

MS. BRAINARD: I'll just interject that, you know, my data point of one, you know, auntie who lives out in Michigan just gets a great kick out of talking to people in India, and just loves it when she gets off the phone. And wow, I just talked to somebody in India. This is real exciting.

Let me collect. Cynthia had a question. I see a question back there. A question over there. A question there. Let's collect all four questions and give our panelists a chance to answer all of them at once and any closing thoughts you may have as well.

MS. JEFFFERSON: Hi. I'm Joan Jefferson [ph.]. I'm a graduate student at Georgetown University. And I just have a question actually for Mr. Lande, where you mentioned that the reason for outsourcing was more so a shortage of labor than--cheap labor. And I tend to disagree with that because I thought the general feeling about outsourcing was that, say, for instance, in China people can be paid 13 cents an hour for work that if it's done here, it's probably going to have to cost companies or corporations $20 an hour. So how do you explain that? Thank you.

MS. BRAINARD: Okay. Over here.

MR. : [Off mike.] I'm Don [inaudible], reporter for [inaudible] Private Computer [inaudible]. And I'm thinking about the fact that class actions are out there as a potential enforcement tool if you will and deterrent effect. I haven't heard anybody talk about it. There's three of them brewing around in California; and other ones elsewhere. The Fair Credit Reporting Act limits you to a $1,000 in damages for each breach or for total breach times a hundred and forty thousand people. That's still not a ton of money to some big corporations. There's talk about making that more. California's version has a $5,000 limit, for example.

I was wondering what you think about the deterrent effects of class actions and, you know, the role that it might play for consumers.

MS. BRAINARD: Question over here, Cynthia.

MS. CROWELL: Well, thank you. You already asked on of my questions. I'm Cynthia Crowell. I'm at the Haas School of Business at U.C., Berkeley. And one question I wanted to ask is if a company who's doing this type of transfer overseas wants to institute best practices, is there somewhere where it's documented as to what these would be, and where would they go to find that?

And then associated with that question is are there any aspects of that that should be legislated in this process? What do you think the pros and cons of that are?

MS. BRAINARD: Okay. And the last question back in the corner there. He will give you the microphone.

MR. SEDIK: Hi. I'm Romaine Sedik [ph.]. I'm with George Mason University. Just to build off of your discussion earlier about the customer's right to know. I was wondering if you would briefly mention what has been the consumers' reaction to the issue of outsourcing. I mean how does the general public feel about it, and also has there been a trend among corporations to outsource portions of their call centers that don't necessarily deal front line with

customers, like personnel issues and things like that that don't impact their profits as much as customer service relations would? If that's something you would comment on? Thank you very much.

MS. BRAINARD: Great. Okay. Let's see on the issue of labor shortages versus cost differentials? Do you want to speak to that, Jeff?

MR. LANDE: Yeah. If I can take a stab at the first and last question since those are tied to some extent.

I didn't draw a distinction between the manufacturing side. For example, the vast cost savings you have of doing work in China, manufacturing beds, manufacturing clothing and such and overseas and software and services. And that's what I was talking about, about the latter one--software and services and in that higher end tech work. You don't have the same kind of cost differential that you have in the basic manufacturing, and there is where we have seen the skills shortages and you've also seen the customization for local markets. And since it's not the same kind of commodity that goods are, it's a very different beast right now.

With regard to the last question about the feeling concerning outsourcing, a few points there.

Outsourcing is a vast category. You know, you can outsource to the business next door, in D.C. Outsourcing is simply taking the function that your business has and giving it to someone else to do. Outsourcing per se hasn't been that controversial.

What has been controversial and has been the topic of great debate for the past 24 or 36 months ha been offshoring, so offshore outsourcing. And there you can do any number of surveys, any number of polls, and you get different results. It's the way you look at it. You know, if you ask someone the generic question, should something be done in America or offshore? Then people will say America in great numbers.

If you ask them are you more concerned about something offshore versus America, the chances are the numbers will say offshore. But when you drill down below the surface, there's really not a good reason for that concern about work going offshore, and when you drill down in terms of quality and such, you have consumers and you have corporations saying that they want this work done where the quality will be best and where it will be most efficient regardless of where it's done.

And also with regard to call center operations, when you really look at this from the standpoint of feedback that companies get from their customers, the ratings that they get really fall based upon where the customer is getting quality results in the most efficient manner and in the most timely manner as opposed to any sort of accent or geographic boundaries.

I can tell you personally that if I pick up the phone and I call someone about my bank account or I call someone about a product that I'm having a problem with, I don't care where the person is as long as they can answer the question. And I think the data bears out that most Americans feel that same way.

MS. BRAINARD: This issue of class actions and the limit on the damages. Evan, Dan, do you want to comment on that?

MR. CAPRIO: I can actually following Jeff's lead sort of take a stab at number two and number three.

MS. BRAINARD: All right.

MR. CAPRIO: I mean the--you know, what's happening in California and with Choice Point, and I assume it's both in state and federal court, I mean that's a--it's a response that--it's sort of a market response. In other words, the company, you know, is and will be punished for bad practices. So, you know, in some ways you can look at that as if, you know, that's the way the legal system is supposed to work and will work, and, you know, where at the

end of the day, you know, costs--I mean presumably there will be some recovery for consumer harm and injury and that, you know, at the end of the day it will come out of the, you know, it will come out of the bottom line.

And that's an important distinction because a lot of, you know, as we've had this panel, a lot of the discussion is about, you know, the movement and the free flow of information, but that where we draw that line is really based on harm.

In terms of your question about resources or where would you go for best practices, I mean what immediately comes to mind is sort of we've referred to both that the OECD has a lot of information about their 1980 privacy guidelines and has worked over the years to--I think they have a privacy generator of sorts that catalogues, you know, different countries and different practices and best practices in different legal regimes. I'd also point you, though, to APEC, the Asia-Pacific Economic Conference, and this privacy framework that we've just recently concluded last November; and that that's--it's an updating, if you will, of the OECD guidelines. And again, it doesn't change the guidelines, but it gives more recognition to the importance of the free flow of information, and it focuses on particular harms in trying to create, you know, a consistent framework, a regime in the Asia-Pacific region. And so there's a lot of hard work and a lot of good information that's gone into negotiating those guidelines, and I'd point you in that direction.

MR. HENDRICKS: Can I comment on that?

MS. BRAINARD: Yes. Please.

MR. HENDRICKS: Well, I think the class actions are--and basically--the private right of enforcement is absolutely necessary because people's rights are not being enforced and until they are being enforced, it's going to continue.

Choice Point, through its testimony, has indicated they're not going to change many of the fundamental things that are causing this problem, and so it's only through--the value of the lawsuit also helps get people under oath and get the truth out of what the practices are.

So I think those are a necessary evil, but until they're successful, we're not going to start cleaning up this mess.

I think on the couple of the other issues, you know, you'll never be able to convince me that cheap labor is not the reason that we're going offshore. But I also agree with you that whether someone accepts a bribe depends on the content of their character, not on, you know, what they're paid, and that I agree with you that the higher up you go, really the worse the corruption is. And we have our American examples of Enron, WorldCom, maybe Halliburton to prove those points.

You asked about best practices. For transparency, I would say look at e-Loan. For fair information practices, look at the 1980 OECD guidelines. There's eight principles. And for security rules that drill down, the GLB security safeguard rules I think are really good.

And the reaction, public reaction, I saw at one time I caught Lou Dobbs, who's on CNN late a night, a twelve midnight, and he's always railing against illegal aliens night after night. I think it's actually rather untoward the way he does it, but I mean--I don't know he's just gone over the top. I don't know what kind of life experience he had, but he's going to be in nursing home some day, and I think he's going to, you know, regret it. You know, thinking of someone who's really being nice to him and taking good care of him, and he's going to ask for their green card or something, you know.

But he did have a poll on that said something like, you know, they asked these surveys, and they said how many people think you should be told if your medical information is being outsourced, and it was 90 percent plus that said that yes we should be informed of that.

MR. LANDE: I add one addendum to what Evan just said, and to the OECD since we're talking about privacy guidelines, but also the 2002, the guidelines for information systems and networks. Those are nine principles. They're societal. They talk about awareness and responsibility. But they're also--of the nine principles four of them are really life cycle in terms of creating this culture security for companies to, you know, do risk assessment, mitigation, architecture, and reassessment. So they serve as a policy framework of sorts at a very high level, but they represent, you know, like the Gramm-Leach Bliley safeguards rule, they represent, you know, an internationally approved document that gives you some sense of what, you know, what good security would look like.

MR. LANDE: Lael, I'm sorry. Can I just offer one other thought that helps me frame this in my mind a lot as I think about this from the standpoint of the U.S. economy and U.S. corporations [inaudible] consumer protection.

This is a global marketplace now, and one thing that I keep coming back to is the world's largest provider of offshore services is actually the United States, whether it's IBM Global Services, EDS, Ford, GE, Perot Systems. You know, we do this work that we're talking about today for enterprises in virtually every other country in the world.

So if we start moving down road the road to really restrict the flow of cross-border data, that is going to turn around and have very significant consequences for the U.S. corporations doing this work elsewhere and their employees.

MS. BRAINARD: Kiran, did you want to also put in a final word, especially on this issue of best practices?

MS. KARNIK: If I may, Lael, just a closing thing, not necessarily best practices--

MS. BRAINARD: Yeah.

MS. KARNIK: --and just a minute. You know, I think Jeff said one part of what I was going to say. The other part which relates to what Jeff has implied is something which, in two parts.

One is I think for all of us as people in this business and this industry, but more important for each of us as a consumer. Privacy is of critical concern, and I think we've got to see working together around the world as this inevitability of data movement is going to be there. What do we need to do in terms of frameworks that are common and that make sure that extraterritoriality being what it is, do we yet have coverage and adequate concern about privacy wherever it is.

Having said that, let me add a bit of an obtuse point, which is very self-serving, and self-serving not only for India but many countries like the U.S. We do a lot of this. Is you know when data moves out of your country, the host country, which is hosting that data, has to bend over backwards to give you that sense of security which I started on the thing in the beginning; that the data is far away. You inherently worry about it. That's it. So they have to make their practices more stringent than what they may be in the home market.

And this race to improve this kind of data security is something which offshoring probably, you know, spurs more and more. We've seen this in India with regard to quality, but our quality of work in India just had to be better than what was being done in the U.S. and U.K. Otherwise, why should anybody come just for cost? Yeah, cost is fair, but you've got to have other things. I mean you're concerned about customer service, market share, sustainability. So you want quality. And our quality had to be better.

And I think the same applies to privacy and data security; that when the data moves out, you want to make sure that it has even better privacy restrictions and privacy practices than what exists then. I think this is going to improve it.

But we've got to make sure the legal framework takes care of ensuring that there are no holes there, and that's whether the data is with the company, with an outside company, or an outside country, and that comment I would make in general.

MS. BRAINARD: Any other final thoughts before we wrap this up?

MR. HENDRICKS: Just that in marketing, they know there's a steak and there's a sizzle. I mean offshoring it brings the sizzle to the issue of privacy. But the real steak is privacy itself and that's a fundamental core issue.

MS. BRAINARD: Any other thoughts? Terrific. Well, I want to thank our panelists for I think a very both informative and well reasoned discussion. Not as many fireworks, which we actually try to discourage here at Brookings.

I would like to encourage you all to visit our site on the Brookings web site. It's the Poverty and Global Initiative. We've had a series of events on offshoring. We've had a data conference that brought together 120 statisticians, and we've got transcripts from that. We'll have the transcript from today's event up within the next day or two. And we've got another big event in the spring that we'll bring a lot of academic papers into this arena as well on the broader issue of offshoring. So I would encourage you to keep looking at the site and I would hope you would join me in thanking our panelists for a very illuminating discussion.

[Applause.]

- - -