

Cato Institute Policy Forum

Should the Technology Sector Support Federal Standards Regulating Online Privacy?

featuring

John Palafoutas, Mark Unacapher, James W. Harper, with Wayne Crews moderating

CREWS: Good morning. My name is Wayne Crews. I'm Director of Technology Studies here at the Cato Institute. I'd like to welcome you to Cato. I think we're looking forward to a really exciting debate on privacy policy on the Internet. Today's the first day of Spring for what its worth, so it's good to kick this off. Privacy policy, tough debate. It's looking less, a little less like we're going to get legislation this year. But one of the curious things here is, I noticed there's a new report by E-marketer, which is one of the less radical reporters, or less radical boosters with what's going on with e-commerce. They indicated that 79 percent of the public, when they encounter a website that asks for personal information, that they simply click away and go somewhere else. Now some may look at that and say, "Well, there's really a problem here, we need to regulate and make people feel more comfortable and more assured about what they do."

So some could see this as a failure, but others could take comfort in that and see a little bit of success there. Because what it means, in a sense, is that regardless of whether you do privacy legislation, opt-out is alive and well. It's happening. People are moving out of sites that they don't think are respecting what their preferences may be. And there are tough problems with what you do on a privacy bill. I mean, obviously those are tough questions. There are different levels of privacy people might want to enjoy. People might want to present different faces to the world depending on where they are on the World Wide Web and even if we, after the campaign finance debate, got through the debate on the budget and got this thing moving, it's not just so simple as to say, "Well, lets have a bill that offers notice and choice."

Things get complex pretty quick, even when you try to do something as simple as that. Because if you apply privacy rules on to the online sector, well what do you do about the offline sector, what do you do about the Safeway Club cards and other things of that sort. If you apply it to the private sector, what do we do about government information collection? I mean that's another issue that's going to come up, either in committee or on the floor. What do you do about preemption of states, who may want to pass their own privacy laws? Some of the A.G.s, are coming to new, Attorney Generals are coming to new compromises in that regard. Problem's over, what about technology? What impact is new privacy legislation going to have on technology and this can occur in a lot of ways. You get a simple notice and choice bill, how do you affect that as the web changes. You know as time goes on, its very likely to be the case that you need to rely on a desktop computer to access the web less and less and you may find your accessing the web through PDAs and cell phones and things of that sort. Well, how do you put a notice in choice policy on a device like that? How do you make a privacy bill apply to what the Internet or the web when you don't know what the web is going to look like in the future, at least in terms of access devices.

Plus there are other technological issues. We know there are third party tools that are emerging to protect your privacy. Some will growl at you or make some kind of noise or do something to warn you when you're going to a site that may not respect your privacy in the way that you'd like, and those tools are evolving too. Well what do we do to the evolution of those tools if governments step in and set those kinds of rules. Those are things that have to be thought about. And also just look at the non-marketing questions. We're going to a world, too, where we've had the business-to-business web, the business-to-consumer web. There was a good article the other day by Jonathan Rauch on the T-to-T web, the thing-to-thing web. If your refrigerator is computing, is communicating with the jug of milk. This is not fantasy. They will be able to imbed chips and palettes of devices, keep track of inventories this way. The technologies are changing so rapidly, and there are others.

Privacy is largely a marketing issue, but there are other areas where it's not like that at all. Consumers will ultimately be able to use some of the same tools to gather information that businesses now use in ways that sometimes we see as not quite so friendly. Even the most worrisome, the web bug, that could let a user or business know that you'd opened an email and that you'd forwarded that. Well, what kind of consumer uses could it have? Well, something like that could be used if you're searching for a job and you need to find work and you need to know if employers have looked at your resume. That's one way that consumers use it. Consumers can use that kind of technology when they send out invitations to parties or something like that. So these are all kinds of issues that crop up when we think about these issues. But we're going to get busy on this debate on: Should there be federal legislation regarding online privacy?

First, let me introduce, first what I'll say is I'll introduce each of these gentlemen just before they speak but we have John Palafoutas from AEA, Mark Uncapher from ITAA, and Jim Harper from Policycouncil.com and Privacilla.org.

And to get us started, John Palafoutas is senior vice-president, domestic policy and congressional relations at AEA, which is formerly the American Electronics Association, one of the nation's largest high-tech trade associations, with over 3500 member companies. During the 90s, he was director of federal relations, A&P Incorporated, where he managed a full range of lobbying activities and management of high tech issues for this Fortune 300 electronic manufacturer. Before that, he held jobs in various capacities on the Hill. He was chief-of-staff and press secretary to Congressman Duncan Hunter of California was press secretary to Tom Wiley, he was a special assistant to Congressman Newt Gingrich. He has a BA from the University of Pittsburgh, where he also did graduate studies in communications research and a Masters in divinity from Gordon Conwell Theological Seminary. And if you'd welcome John Palafoutas.

PALAFOUTAS: My able assistant will now press the right button. There it is, you're set. The difficulty in today's presentation is going to be that I'm going to end agreeing with everything that the other two people have said. It's the frustrating part of this debate on privacy. However, before I start, is Chris Mustane here from IBM? Okay, good. I don't have to be quite as careful then. He's really smart and I'm always intimidated.

Let me give you a brief overview of AEA and how we came to our position. AEA has about 20 offices around the country. We're a rather broad-based industry group. Back in January of 2000, what we call our state policy action network. Our company people lobbying at the state level said we're having a big trouble in the states because we're going in and saying, "No, no, no," on any kind of legislation at any level of government and we have no lobby tools to use against the state legislators. We need you to come up with a position for federal legislation. At that time, we rejected that idea, but by October of that same year, our Board of Directors brought this up, who are a group of executives, senior executives, CEOs in our companies, and they brought up the issue that said, "We need to come up with a privacy position and we need to come up with a position that reflects the reality of what's going on in Congress, at the state level, and in the marketplace.

This is ADA's position: We support the adoption of federal preemption legislation that is consistent with the following guidelines and I gave you a press release and I notice that some of you who were bored enough to even read it before, as you sat down. We believe that there should be federal preemption language. It's a position that we believe is a realist position, on several fronts. It's a realist position in terms of consumers. We believe that our first responsibility is to consumers and consumers have a vested interest in these privacy issues and we're going to hear more—I'm very interested to hear what Jim has to say on this because I'm afraid he's going to completely obliterate my arguments but I'm still going to come out with the same position. Mark and I have been doing battle by dueling press releases now for months, so this will be an interesting time. But our position is we need federal preemption language. For the consumer's well-being, and, I would remind you, given where we are, it is in some respects, the libertarian position. It's the limited government position. We're saying that we can't have 50 state laws governing privacy. And the way things are going on at the state level, that is one of our biggest concerns.

Now the context for this decision. Last year there were—wait a minute, I'm going to have to back to that one. That's the context for the position. There were over 300 bills introduced at the state level, and in June the National Association for the Attorneys General met and had, what we considered, a pretty onerous policy. They have since that time backed off. The situation in 2000, we believe in 2001, is that privacy policy is going to be a pretty big issue. Now I'm going to have to back to one.

It's important to understand our assumptions at AEA. The first assumption is nobody else is more concerned about consumer confidence than our companies. We believe that's central to the issue that our companies are more concerned because if the consumers lack confidence, we heard what Wayne said, if people go on/out to a site, and people start asking for information, they opt out. They just get out of it but our companies want people to get on their website. So they are the ones primarily concerned with consumer confidence. The second one is just as important in the sense of this. Privacy is an emotional issue; it's a confusing issue. I once, last August, said at a conference that the American people are hysterical about privacy. A reporter came up to me afterwards and said, "I really take umbrage with what you just said. My wife's personal identity was stolen. It took us a year and a half..." And for the next five minutes, he let me have it. And at the end of it, and he says, "Well, what do you have to say?"

I said, "I'm right. You're hysterical about it. Your issue has nothing to do with personal privacy. It has to do with security." And you'll see this today in today's *New York Post*. Actually, it was the top story in CBS radio news, was this whole cyber-fraud where a busboy in New York managed to get financial data on the Fortune 400 and went down and evidently made a lot of money from this.

Well, what's going to happen is that this is going to migrate into a privacy issue. And this is the problem we have in the industry and with members of Congress—that confusion. And for us in the industry, and I think this one place where the industry has failed, we have not adequately educated members of Congress. We have to deal with that reality, and you take that also at the state level. Members of Congress today are not surfing the net everyday. They don't know what a cookie is other than an Oreo, they don't know about the technologies that are out there. They're not focusing on this the same way the industry is. And this is the scene we have to go into, the whole milieu we have to go into, is we have a lot of ignorance and a lot of confusion about it.

And just so nobody gets on my back about the hysterical argument, I'm hysterical about privacy. I mean I have an emotional antipathy towards the Safeway card. And I watch people go in and I'm paranoid about it. I go, "Aha! They know you bought applesauce! Now what's going to happen?" And for some reason, it makes sense to me. But you know, people swipe those cards everyday. But that's the issue for a lot of people, is that there's something wrong about the information going on the net and that activity occurring at light speed. And people are nervous about it.

I talked about the members of Congress not understanding the technology, the other is, political pressure will increase. The story today in the *Post* and CBS News, there are going to be other stories. All there has to be is what you call the Privacy Exxon-Valdez to go on. Where some little kid is hurt or somebody's defrauded of a lot of money and left homeless on the street because of something that goes on the net. All you have to do is put privacy on top of that and it's over. Members of Congress will not be able to withstand that kind of pressure. And at the state level, it's even more intense. We forget in Washington the state legislators have a much greater interface with their constituents than they do here in Washington. They probably have a business on Main Street, they're probably not full-time legislators and somebody's coming in and saying, "Zeke, what are you going to do about this? This is awful!" And so state legislators are ready to act even though they don't have all the issues in front of them. The other reality, assumption I'm making is members of Congress I hope in some respects—Wayne's correct that Congress will slow down about legislation this year—but I don't have confidence in that and that's probably one of the critical factors of AEA's position.

We met, several of us met with Congressman Sterns, the subcommittee chairman on the Commerce Committee who is going to introduce legislation in June. Congressman Tauzin has asked that we have some consideration in the Fall. Now, that doesn't mean it's going to happen but the train is moving and we believe that legislators are going to have some options out there. And legislators are not going to be able to answer the questions about what are you going to do about privacy? And what's going to happen is legislators said, "You don't have to worry. The companies are really looking after your better interest."

That argument was made yesterday in a discussion we had on yesterday on Capitol Hill. It did not resonate. Members of Congress, for good or ill, have to do something. And they're gonna either pass a commission bill, they're gonna pass some kind of legislation to go into that vacuum that seems to be going on now.

I'm not going to go through each of these slides in detail about the states' bills, because it bores even me, but I want to give you an idea of what's going on. California last year had a bill, had private right of action. Which basically is individuals have the right to sue the web provider, which is a horror show, and which we can talk about later and I'm sure some of our, I think Mark might even talk a little bit about that. It'll just get to the point where he talks about private right of action, I probably agree with everything he's got to say. That ended up in the bill.

Washington State toyed with a ballot initiative, which would have been terrible. We saw in these states also initiatives last year. Maine had a particular interest. It wasn't the Internet, but they had an interesting medical privacy bill that shows the law of unintended consequences. They passed a medical privacy bill because consumers were asking for some kind of protection. What happened after the bill passed, is you had scenarios where by in one incident a woman got a call from the police, said, "Your husband's been in an accident he's at Augusta Memorial Hospital. You should get over there right away." She shows up at the hospital and says, "I just got a call from the police. My husband is here," and the clerk at the front desk says, "I'm sorry that pertains to protected medical information about a patient. We can't divulge that."

"Well, can you tell me where my husband is?"

"I'm sorry we can't give that information."

The priest shows up. One of his parishioners asks the same question. "I'm sorry we can't give that information." Flower deliveries come. "I'm sorry we can't give this information." Within a matter of months that bill was overturned, again, because of the law of unintended consequences.

The fact that a few states have been slapped on the wrist metaphorically doesn't change the fact that I think we're going to have even more legislation here. And a good example is what happened last week in Georgia, there was a Database Protection Act introduced in Georgia. A state senator, a committee chair, and the governor decided to put in privacy language. It's innocuous on its face, however the lawyers, and I'm sure both the lawyers and the panelists I'm proud, I'm not sure I'm proud to say, but I'm not a lawyer, and I'm going to stay an ignorant layman on this case. But this language looks pretty innocuous and it's why the state senator and the governor felt pretty confident about putting it in because it was so innocuous. This starts to unravel immediately. When you start to—well what are the definitions, who's going to decide if the notice was proper? Who's going to decide if this was really the proper use for which this information was gathered? And it really got down to each of the county judges would be the arbiter of this, and if this had passed, this would have become a de facto national standard because anyone who could access a database in Georgia would have been subject to this. Then you get into questions, well how is it enforced? So, the issues are starting out already. And if we

have state laws and especially some of the big states, and actually Georgia is a big state for high-tech. But Texas, California, Washington State, Colorado, New York, Pennsylvania, Michigan, any of these big states pass laws, they'll become a de facto national standard and that's something that we at AEA are extremely concerned about.

Maryland had a Consumer Privacy Bill. I think Mr. Uncapher testified there last month. They called for notice to opt-in. Again, we believe that consumers should have choice but we don't want the government to telling either industry or consumers how that choice should be adhered to.

Massachusetts had a bill. Again, with these particular provisions. Now, the issue, the state that gets the industry concerned is often Texas and California. We'll go to California in a minute. Texas has this initiative, probably the only thing that's going to save us in Texas is that they just don't have enough time to deal with the bill. Come, I think, early April, they have to start dealing with redistricting and it's going to slow down the whole process of other legislation. But if Texas passes something, it's going to have great implications. Now, NAG, the National Association of Attorneys General surprisingly, I thought, came out for a different policy than they had initiated last year asking for enforcement authority from the federal government. That was a big change from what we had anticipated their coming out.

Now California is problematic on several levels. One, just because it's California, and they think they're another country. The other is State Senator Steve Pease and for those of you who are theologically minded, I think you cannot overlook the significance of the number of his bill, for goodness sakes. But the beast referred to in Revelation 13:18 with the number 666, the antichrist, I'll let the journalists finish the line. But Senator Pease, as you recall, was the author of the California State energy so-called de-regulation bill. He's now going after privacy and in remarks he made to our remote policy action network in Silicon Valley in January, he spent an hour and a half of a dinner speech, and this was prior to us eating, like it is for you for lunch (but you're a little earlier), but an hour and a half comparing the energy de-regulation to privacy. It was probably the most frightening rhetorical 90 minutes I'd ever gone through. But this is the problem we have in the industry and what's going on at California. So, despite the fact that, as I said, I'm probably going to agree with most of what my fellow panelists say, the conclusion is going to be we can't have confidence that the states are not going to take action. We believe that the consumers will be hurt and the industry will be hurt.

You have the press release in front of you with our principles that we will look to evaluate legislation, and there's going to be legislation. Senator McCain has said he is going to put something in with Senator Kerry; we'll probably have the widened Burns Bill. We certainly have Senator Hollings in with the bill. Congresswoman Eshoo and Congressman Cannon have a bill in and we're going to have the Commerce Committee bill coming up this year and these are the criteria that we'll use to evaluate them. The big issues for us are choice, notice and the other issues we have up here and, as I said, if Mark doesn't cover some of the details, we'll cover them in the Q&A. But to show you the difficulty that we have with the issue, even in dealing with the industry is this next statement on uniformity.

In a network economy, the exchange of information is an essential component to commerce. The interests of the Constitution's Commerce Clause are served by having uniform national privacy rules. Now, this is something that we at AEA as an organization of individual companies agree with wholeheartedly. Now the trouble is it's ITAA's position and they've come out against a uniform privacy, or preemption at the federal level [Huh? Oh I thought you'd like it]. It's the problem we have in the industry. We all want uniform standards. The question is how to get there. I'm looking forward to Jim's comments about the Commerce Clause just to help us to get there. But we believe the only way to get there is through preemption language at the federal level, understanding that a great deal of mischief and the devil really is in the details. And now I'm looking forward to hear what Mark has to say, so thank you.

CREWS: Okay, thank you. Our next speaker is Mark Uncapher. He's Vice President in Counsel of the Information Technology Association of America, responsible for ITAA's Internet Commerce and Communications Division, which is just one of four membership divisions within ITAA. Members include Amazon.com, AOL Time-Warner, AT&T, Boeing, Cable & Wireless, IBM, Metromedia Fiber, Microsoft, and many others. Mark was formally counsel to the Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform and Oversight where he was principal staffer for the Subcommittee's hearings, oversight activities and committee report on the problems associated with the Y2K computer problem. He was also the principal committee and floor staffer for the landmark electronic Freedom of Information Amendments of 1996 and for the Family Privacy Protection Act, which was part of the Contract with America. Mr. Uncapher served in the Giuliani administration at the New York City Department of Homeless Services. He's worked in the broadcasting industry as an executive and the broadcast division of Park Communications, the Newspaper and Broadcasting Group, and Sage Broadcasting. He's also a founder of Mattatuck Communications, a privately-held station owner. Mr. Uncapher is a graduate of George Washington University and the New York Law School. Take it away.

UNCAPHER: I was going to start out by saying that John and I agree on an awful lot of the principles we have and also our assessment of the broad challenge that we as an industry face on privacy. I think it was particularly driven home to me when I saw television show that had identified the villain as some corporation that had some kind of scheme or some plan to take people's privacy away and the good guys were going to go in and try break it out. So we've reached the point in the privacy debate of being villains. You know you've got to, we've displaced neo-Nazis and Arab terrorists and so forth and so on.

The point of disagreement though, the conflict I think, is really on what the prospects are for federal legislation and what the possible content of federal legislation is. So sort of we agree with all the premises building up to that, but where there really is some disagreement is in kind of looking forward to what Congress is likely to do. Our fear, the fear of our companies, is that in looking out at the states and trying to get federal preemption, which would be a laudable objective, there ends up being a kind of, if you will, in the consumer context, a kind of bait-and-switch, where we think we're getting federal preemption and we're protecting the Internet commerce from a lot of state laws that would have a negative impact, but instead we end up getting, as an industry, considerably more onerous legislation. It's worth kind of stepping back and looking at some of the laws, some of the proposed laws that are out there.

In particular, John mentioned private right of action in a number of the state bills. Actually, there's a private right of action in the Hollings Bill, which has, or had last year when it was introduced, some ten co-sponsors, many of which are members of the Commerce Committee. Private right of action, again, basically it's not the FTC, it's individual lawyers bringing lawsuits would have some \$5000 of damages in each violation. Again, there's not any requirement to provide the kind of harm the threshold is set at \$5000, which of course could be multiplied towards a number of individuals, or so forth and so on. Now, you may say, "Well, no wait. That's just if it's a really bad situation. That's when they can bring that \$5000." Now actually if the provisions go on and says if it's willful and knowing violations, it's \$50,000 per violation. So presumably the \$5000 just applies to innocent violations. It goes on, I mean, there are other provisions, there are protections for whistleblowers so that I guess if an employee was involved with a privacy violation and leaves and gets whistleblower status then they're protected. There really is a lot to be very concerned about. And this is, if you will, in the privacy debate on Capitol Hill sort of one of the poles that's out there, one that has attracted considerable support.

Now I know that others sort of look to the McCain-Kerry Bill as being maybe something that's more minimal in the notice requirement or sort of more acceptable in something that would satisfy this concern about being able to preempt state law. Again, the McCain-Kerry Bill, the one that was introduced last year, now they haven't done one as yet this year, but the one that was introduced in the last Congress has some fairly complex notice requirements. If you look at it, it's rather detailed in terms of what websites would be required to do. It requires it to be "clear and conspicuous" and easily understandable.

We'd argue, first of all, "clear and conspicuous" is a text-based standard that belongs in the world of newspaper ads where you're regulating font size, it really doesn't apply in the online world, but part of it is there that there's this conflict between having something that is clear and conspicuous and understandable and then also contains a fairly detailed set of requirements as to what goes into the notice. We'd also criticize the, again, this text-based standard we'd argue that with the P3P implementation coming up later this year with Microsoft comes out with the Explorer SP, and as Netscape comes out as well, that the consumer tools will be available to do a much better job of communicating privacy policies to consumers than these mandated text-based standards of the consumer who could set browser for particular preferences and then get alerted on a case-by-case basis when they go into sites as to whether or not they adhere to their privacy preferences. And again, there's nothing in the McCain-Kerry Bill that provides any kind of safe harbor or carve-out for being able to communicate the policy in that way.

So in a sense, what the consumer has to do is go read the sort-of privacy equivalent of a mutual fund prospectus and go read to see if it hits those particular preferences. Again, I would argue that the marketplace with the technologies is doing a hell of a lot better job than the notice requirements that have come up in statute. So again, we kind of have Hollings out here, and then maybe McCain out here, as opposed to the principles that we would agree on of being over here, kind of a more simple notice.

I should say one thing, too about the McCain bill on the damages. Fortunately, it does not have a private right of action, and for that, I think it's positive, but it does have a \$22,000 per day penalty per violation. Up to a cap of say, a \$500,000, where it's capped out.

Now, our concern on the issue, and we would share with AEA, is this notion of technology neutrality. In effect, what this would mean, as I would read it, would be that a site, let's say a restaurant in a strip mall could put up a website and collect information for a drawing, you know the equivalent of drop your business card in the fish bowl and you get a free dinner. If you collected that information online, just name and address and so forth, and so forth, you would be required to have those kinds of notice requirements. Now, if you made the mistake, and I mentioned the strip mall, if you made the mistake of not providing adequate notice on third-party sharing of information, again the McCain Bill is very specific and very detailed about you can't just say, we might share information with third parties. It's fairly specific about how that gets done. That little business coming online in e-commerce would be running \$22,000 per day in fines, and after about three weeks it would be up to about \$500,000. I'd argue that that's wildly disproportionate, but of course that's what one of the problems is. These bills tend to have penalty clauses that have no bearing whatsoever to the damages involved, which is a real concern. I mean, if one of our principles, uniformity is certainly one of them, but one of our principles is with proportionate penalties.

I contrast all of this, I mentioned P3P, but I'd contrast all of this is to what the industry is already doing. I understand the considerable public outcry about the issue. I'm also very conscious of the activities that are existing at the state level. But bear in mind the most heavily trafficked sites in America have voluntarily put privacy policy up on their website. In response, it's not frankly because of policy, it's because of marketplace pressure, but they've voluntarily done that, which is something that has real world legal consequences for them. If they violate those privacy statements, then they will be committing an unfair deceptive trade practice, which would be actionable on the FTC. If they did the exact same thing but didn't have a privacy notice up, there would be no liability. So the marketplace is very clearly responding. And again, it's not in dispute that the overwhelming number of heavily trafficked sites have those privacy notices in response to the very real pressure. I would add, that once we get to the technology tools and they're able to communicate those notices more effectively, than through P3P, that we'll be able to have a more robust dialogue with consumers that really drills down to their individual preferences and let them control what they do and what they don't.

I have a Safeway Card, frankly it's a pretty good deal in terms of the discounts you get, but that's a matter of personal preference. My phone number is also in the phone book. I haven't opted to have unlisted number. I probably get a few calls as a result of that, but clearly, different people have different preferences, and a single law is not going to be able to accommodate that kind of range of activities. What's more likely to do that is to give consumers a variety of tools and allows them to decide for themselves how they want to exercise their personal privacy preferences.

A lot of this issue, I'll conclude by noting that goes back to this sort of process of adoption. We've come online, we've adapted, we've gotten involved in this technology extraordinarily quickly. Internet commerce is really only a handful of years old. If you compare

it with other new technologies, it has come, it has been adapted by the mass market much quicker. So candidly we are running into much quicker as consumers as we are kind of experiencing elements of personalization for the first time, a kind of sense of creepiness and we weren't expecting it.

I like to use the example, it's not an online example, but the first time I put an ATM card, my bank card into an ATM, and I got back on the screen, "Hello, Mark Uncapher," and I gotta say that was kind of creepy. My god how did they—and then of course, duh! I've put a card in with my name on it. There are lots of examples of this where there's an element of personalization that is unexpected when consumers reach that for the first time that is a little bit creepy. That is disconcerting. That catches them unaware and is part of that sense of things being out of control or that unease that consumers have that is the underpinning for this whole privacy debate. There's this sense that my god, there's this sense that these databases out there, what do they know about me?

I would submit, that in time, as the privacy tools come online and people have a better sense of how to navigate through the process and also, as they become more use to operating in the e-commerce environment, that the equivalent of the Amazon site, which gives me my preferences and makes some suggestions about possible books, that will be perceived as being a benefit, as opposed to something that needs to be addressed in legislation. Thank you.

CREWS: Thanks Mark. Our next speaker is Jim Harper. Jim's the editor of Privacilla.org, an online privacy think-tank, and he's the founder and principal of PolicyCounsel.com. Previously, Jim served as counsel for the House Judiciary Committee, as counsel to the Senate Government Affairs Committee, and in several other roles on and off the Hill. Jim's a California lawyer, a graduate of Hastings College of Law, and the University of California at Santa Barbara. During law school, he was the editor-in-chief of the *Hastings Constitutional Law Quarterly*. And I'll add too, that on Jim's policycounsel.com website, if you click on his photo, he starts making faces at you.

HARPER: Thank you, Wayne. That was a trick that I put on the Policycounsel.com website to see if people are paying attention to what kind of links there are available there. Wayne's obviously very technologically savvy, so he came across that stuff. Now the cat's out of the bag.

From the real political perspective we got from John Palafoutas and the technological market-based approach that Mark Uncapher put out, I'm going to go to the abstract and theoretical approach, that I'm entitled to do as a privacy advocate. At some point, it seems that privacy advocates are allowed to say just about anything they want, anytime, depending on what audience is willing to hear it.

Well, let me say first that I'm very pleased to be here at the Cato Institute speaking in this room. I've spent a lot of time sitting in those seats up there during a number of very interesting programs that are put on. I've looked at the list of folks who are here, and between the audience members and the panelists, I think we could spend another 30 minutes on this, get privacy figured out, and then go have lunch, take the rest of the day off and pretty much wrap it up from

there. If that's not appealing to you, maybe we should go to straight to cocktails and then call the privacy issue settled.

Let me tell you briefly about Privacilla first. It's a project of my lobbying consulting firm, PolicyCounsel.com. I intend to incorporate in separately and go for 501c3 and all that kind of thing, but it is a project of a for-profit firm. I represent and consult to clients not specifically on the privacy issue, but you can't deal on any issue these days without it touching on privacy in some ways, so I think it's important for you to consider the potential bias of what I say and the potential bias of Privacilla itself when you look at the site and listen to what I say, as you should with any resource, any privacy advocate.

Privacilla has been described as privacy-policy portal and as online think-tank, and I think those are both good descriptions. What I've tried to do with it is I've tried to assemble information and links on all elements of the privacy issue: Government and privacy, private sector privacy, including financial, medical and online. The law that applies, what laws should apply, current issues, theories, just about everything you can get. At this point, Privacilla's about 180 pages of just text and length, homemade HTML, which is why it looks so darn bad, because I do the coding myself. And I think that over the course of the year it will probably triple in size, and only then will it begin to actually satisfactorily address the issues and all the nuances that can be done on the privacy issue. If there's one thing I've discovered through my study of privacy, it's how little I know, even though I could spend all day, every day studying the issues. It's deeply, deeply complex and obviously it's important to focus on the political here and now and work on the technology.

One of the things Privacilla attempts to do is dig deep down to those fundamentals. The motivation for me to do it was sitting on the Hill as a staffer watching the privacy debates going on and watching privacy legislation passing without ever getting a sense that people new exactly what we were talking about in terms of privacy, what it is. I'm actually going to come back to that and spend a little time on the federal legislation question, which is today's particular issue.

Everybody has their prognosis for federal legislation. The quotable line I have on the prognosis for federal privacy legislation is that, "Since last fall, it's been retreating faster than Iraqi troops during Desert Storm." That's S-T-O-R-M. We heard in the Fall that we'd come out of the gate in January with legislation and that it would be the first thing to move and there would be hearings and so on and so forth. And I don't want to be calling anyone's bluff, but I think as staff and legislators looked at this issue more carefully, they realized that the debate remains essentially incoherent and that to move legislation would actually betray what's in the best interest of consumers and the best interests of the economy in the country. So the time remains ripe for us to think further about privacy and what privacy legislation is appropriate.

Certainly there are privacy proposals that could pass and I think one of the lead questions is whether this approach where a federal regulatory standard is accepted by industry and exchanged for preemption of state laws. I think that's one of the leading approaches that have been discussed. So I just want to discuss that one again from a slightly more theoretical level. I think the premise of the deal that's encompassed by that legislation in a legitimate one. It would be no surprise to me to see the states being adventurous and perhaps foolish with privacy

legislation. I think the example from Maine is a very good one, where they attempted to help privacy regime that failed quite miserably. Some I'm sympathetic to the concerns of the tech industry with what's going on in the states but I think that what AEA, in particular, and that sector of the tech community wants to get done, is actually already taken care of the dormant element of the U.S. Constitution's Commerce Clause.

The dormant Commerce Clause, for those of you who aren't nerdy Constitutional scholars, is a court-created doctrine that strikes down state laws that interfere with the national marketplace. Under essentially three different theories the dormant Commerce Clause strikes down laws that have too great an effect outside their own territory, and John mentioned one specific example of that. It strikes down laws that burden interstate commerce disproportionately to the benefits accrue to in-state consumers. Third, it strikes down laws that create inconsistent state laws if each state was able to pass its own privacy regime.

Now I'm not equipped and there's not time to do a full analysis of how the dormant Commerce Clause achieves the goals that AEA would like to achieve, but certainly that analysis needs to begin because the concern is, you know, the tech industry will invite static regulation on itself in order to get benefits that already accrue to it through the dormant Commerce Clause that the Supreme Court has put forth as an interpretation of the affirmative Commerce Clause that Congress typically uses.

Now I want to turn to why I can be so blase about no privacy legislation happening at the federal level and privacy legislation being affirmatively struck down at the state level. And that's where we really get into some theory and the sub-straight of the privacy issue, which is something that I think everybody still needs to be considering.

Like I said, I started Privacilla because I see fundamental flaws in how the privacy debate is proceeding and I want to illustrate one of those flaws using hypothetical that you all might find quite disturbing. Because in this hypothetical, I've been elected President of the United States with such a mandate that I can pass any law I want to and the first law I'm going to put forward is called the Consumer Happiness Protection Act of 2001. Under the Consumer Happiness Protection Act, your happiness is guaranteed because I will make it illegal for anyone to tell you bad news without your permission.

You probably think I'm going to go down the First Amendment line with this, and there is plenty down there. But in fact, I just want to know how many of you think you'll be happier under a legal.....[tape ends]...Purports to directly give you happiness. What governments are in a position to do is create circumstances. Life, liberty and the *pursuit* of happiness. And happiness, like privacy, is a personal condition. It's a state of being. A lot of people have searched around for a definition privacy, and I'm still searching. I'm not going to claim here today that I have the right answer, the final answer. But my best assessment at this point is that privacy is a condition that people enjoy, or when they lack it, fail to enjoy. Any claim by a government that it's going to deliver privacy or happiness is an empty claim and it's a fake. In the area of privacy all governments can do is establish secrecy or confidentiality that represent the guesses of politicians and bureaucrats about privacy would look like if people were actually able to exercise it.

Now, in a country like ours, where hundreds of millions of people are making billions of decisions everyday that affect what happens with their personal information. The guesses of politicians and bureaucrats cannot possibly, possibly accommodate the actual privacy preferences of consumers. The way to protect privacy is to distribute those decisions to the people who are affected by them the most. Empowered consumers are the ones who will deliver privacy to consumers.

Now, when I say empowered, I don't mean empowered by government-mandated check-offs, I mean empowered by how knowledge flows in our society and empowered by the right to contract for levels of protection for the information that they want to share, or that they want to keep to themselves—that kind of thing. It's certainly not easy. I'm not offering the simple solution; that's not my role here. But it's empowered consumers and there are two things governments can do to empower consumers, two obvious things (and there may be a few more). First, they can stop from actively eroding the ability of people to control information about themselves. There's been a lot in the press recently, and Privacilla has issued reports making the case that government is very much in the business of undermining people's ability to protect their information. I think it's fair to say that privacy is a cost of government. That doesn't mean we stop the world, I want to get off because, and stop every program, but privacy should be considered as a cost of all government programs that, for example, tax, and require financial information. Or give benefits or require people to share medical information and so on and so forth.

The second thing government can do is circumstances in which people protect privacy at the levels they want. This is done essentially in two ways: by enforcing contracts, and by enforcing the law of privacy torts, both state level laws.

I think more importantly than that, though, is consumer education. Consumer education is the lynch pin and it is largely the responsibility of the tech industry if they want people to be comfortable in the online environment to educate consumers about how the online environment moves. I think John may have admitted, yes, the tech industry has not done all it can to do that, or since Swindle makes the case constantly to the industry that it needs to educate consumers and work with them, and I'll just repeat that. I think it has to be on, I think it's the responsibility of the industry, and not of government because the industry stands to benefit. There are companies with billion-dollar market caps that stand to have even more billion dollars added to their market caps if adoption of online technologies is full and robust. If there is going to be a federal rule in creating consumer confidence, my thinking is that the Federal Trade Commission should be responsible for educating consumers. If it can't drive privacy pole numbers down, it should lose funding because it is unable to educate consumers in a way that would make them comfortable in the on-line environment, although I don't necessarily endorse the FTC even taking that role at all.

There's plenty more to be said, of course. We actually won't get it done in the next 30 minutes. But I think Congress can do little to protect real privacy, nor can state legislatures, unless we want to reinterpret privacy as some sort of information age entitlement. What Congress should do, and I think it's in the interest of the tech industry and the best interests of the economy, and it will not erode privacy, is Congress should codify the dormant Commerce Clause

cases so that the protection for national markets implied in to the Constitution by the Supreme Court is finally perfected. There is no need for the technology sector to invite federal regulation in order to get protection that existing law already gives it. I look forward to the questions.

CREWS: Okay, we can now open it up for questions. I'll start it off with just a quick one. One of the criticisms that is out there about privacy legislation is often those who advocate privacy laws will say access is important, access to the consumer's data. What are the dangers of relying on that? Are there security measures or security risks in allowing access in that way? That is one of the criticisms I've heard.

***I don't know what the criticism, what's the criticism made?

CREWS: That consumer access to that data can lead to holes, kinda the security holes that...

***Well, it's virtually impossible for consumers to get access to all the information anybody has on them. Lets start that. General Motors has 100 websites and they're all managed differently. Phillips Electronics has about 75. Oracle has websites. So, the question is, when you go for access, where do you go for the access, what responsibility does the provider have in allowing you access and access to what information? Sears is a good example. If you go to Sears, you buy a refrigerator in one city, you buy a stove in another, I mean, there's warranty cards all over the country about you that give information. Do you want all the access, all the information that Sears has about you? I'd argue, and I think the industry would, a lot of people, what do you care about all the information that Sears has on... and some of these other places. What you want is, when you find out that there's a problem with some information that is detrimental to you, that you want to be able to get to it. When you get to access, you're into huge problems, not the least of which is warranty cards. Motorola has hundreds of thousands of warranty cards out there. Do you want them to go through their warehouses to get this little warranty card you filled out in 1973 on some phone and say, "Aha! That was really material to my life." So, there's huge problems there.

CREWS: Do you guys have any comments?

***A lot of what you hear about in the privacy debate is actually focused on other issues. It might be nuanced other issues, but they're often other issues, and access is very much a different issue from privacy. If you were to take everything you knew about me, let's say a company were to take all its records of me, seal them in concrete, and weld that into a 50 gallon drum and drop it into the deep water ocean, my privacy would be well protected in the sense that that would be not accessible to anybody. Nor would I be able to access it. So, I think that demonstrates the difference between access and security. It's underwater a mile deep; it's very secure in my privacy in that iteration of the information is very well protected, but I don't have access. Access serves a lot different purposes and some very good ones, but it's not about privacy necessarily.

***The example that was used before about the main law or the spouse that was trying to get into the hospital provides kind of a concrete, concrete is, I guess, the right word, concrete example of the conflict between access and security. There are times when you want a third party to be able to have information but there are also times when you want to be protected and it

requires a sort of balancing of the tradeoffs in that case. The same set of circumstance could have been an estranged spouse comes in and tries to get access to the information and as a result of that gets information that they're not supposed to do. Organizations, companies need to be able to have some discretion in being able to balance that. Most companies I know would love to get an updated address when you change, they're only too happy to make those kinds of changes. Its kind of when they get to these other issues where there's a level of protection. The real fear in some of these access requirements would be that it would be harder for organizations to protect information that, a little like the example in the newspaper today about this person who was able to pick out information from a variety of sources in an identity theft situation that they'd be able to do the same thing by again, doing things, lets be very clear, already illegal, there's not a need for there to be a law, but by using pretext to be able to put—piece together information will allow them to do things that are illegal. This is an area where there really is a conflict and there really needs to be a balance. And that trying to get it right at, sort of, a 50,000-foot level that mandates one or the other would fairly dangerous.

CREWS: Do we have a microphone for the audience? Do we have a microphone?

***I'll say, while the microphone moves around that there are a lot of issues talked about a privacy and certainly one of the biggest ones is identity fraud, or identity theft, which is a crime problem, and I think needs to be addressed seriously as a crime problem. It has effects on people, and they're very upset by it, but the majority of the problem is crime, just like an assault and battery affects one personally very intensely. It's not a privacy problem. It's a battery problem and identity fraud is a fraud problem, better characterized as that than a privacy problem.

CREWS: Drew?

DREW CLARK: Drew Clark with National Technologies Daily. Jim, let me take you up on your question or offer to consider privacy as an information age entitlement. Let's just set aside cost for a moment and ask the theoretical question: What's wrong with a rule that says customers must be given the right to consent before their information is used? In other words, an opt-in approach, you need to get consent. I'd be interested in the reaction of all of you. What's kind of Constitutionally morally wrong with the very intuitive idea that a company shouldn't be able to share information about me that it has collected about me unless I've given my consent. Sure, they'll need to re-engineer all their systems to do that, but by going forward from now on, what's wrong with that rule?

HARPER: I agree that's an intuitive rule. I think consumers already have that option if they're willing to exercise it. It's by no means perfected, this option, and I think the business community needs to step up and make it more available but the ability to withdraw from transactions, to hit the back button on your browser. It's more powerful than people realize. We do it all the time, everyday. I'm one of those people who gets to a site and sees that they want too much information for what they're going to give me, and I'm outta there. I'm gone. The idea that the government should step between this transaction is sort of a shortcut that I think would tend to disempower consumers, suggest that they're not responsible for their information, and in fact, what is going to deliver privacy is, as I said, is consumers making those decisions. So there's an

element of personal responsibility that goes in there. So the idea that there's an intervening step where the government has to mandate that option being given. Consumers can mandate that option being given and they're doing so. I think I don't like to decide between opt-in and opt-out. Those things are good business but they would be bad law.

***I think one of the things that technology tools looking forward have the potential is perhaps making the choice about opt-in/opt-out a little bit less stark in the online environment. I'd submit that with P3P if you've adjusted your browser to set your preferences you can have, in effect, an automated dialog that lets you make the choice, opt-in/opt-out under particular circumstances or when, you know, sites meet a particular set of requirements and I think that offers considerable hope in the debate. But before we read, and candidly something that's not reflected in the law so far, but even short of that, I mean businesses are looking not for people who are not interested in information; there generally is some kind of nexus of presumption that there's a probability that people who are getting information are interested in that information and generally speaking that's something that consumers respond to. It really is a fairly small percentage of the population that would be argued that have been called kind of the privacy fundamentalists that have those kinds of concerns with sharing of information. There probably just as high a percentage of people who would be annoyed at what they would call, you know, the "annoying drop down boxes" that would force them to kind of affirmatively opt-in every time. So you've got to balance it. Yes, there's a group of people who could exercise the restraint that Jim suggested in sharing information but you know, the requirement of opt-in would in effect penalize those people kind of know what they want and don't want to be bothered every time with this kind of nanny that says, "Hey, are you sure you want to give that information?" People can decide that for themselves.

***The big issue for us is choice. And why should the federal government be telling you, as a consumer, you, this is the choice option that you have at this particular website. And you were kind of cavalier about it. All they have to do is go back and reengineer their whole system. Yeah, okay, just like that. We'll go reengineer it. There's a movie out, just was out I guess last Fall, *What Women Want*, was Mel Gibson thing. Fascinating movie. The industry should make a movie, *What Consumers Want*. Consumers want, you know, inexpensive things that fill their needs, that do all sorts of things, especially on the first, they want it inexpensively. If you use the opt-in out of context, it can raise prices, it can do an awful lot of things and it can't really give consumers what they want. I think that's an issue and a decision that a particular vendor or company makes with a particular consumer. When the federal government gets in it, there's a good chance they're going to screw it up. But you also have companies that right now have already gone for the opt-in, you know, some of the telephone companies. They already have an opt-in principle. The decided voluntarily to do it, that's what protects their consumers and why they think it's the best way to deliver a product and think that's where we should leave it, in the marketplace.

CREWS: Maybe one of the risks in privacy rules is that minimal legislation would presumably be an opt-out rule, where you just check the box and you don't want the information used but that would be something easy to turn later on into an opt-in requirement and part of the risk there is opt-in requirements could have First Amendment ramifications. When we deal with businesses we talk about them, businesses deal with us, presumably they have the right to talk about us too.

Can we control their speech in that regard and where does that go if we have those kinds of opt-in requirements in place, can they apply later to journalists? Can we control what gets done with the information? Part of this up to that theoretical debate, too, that Jim was talking about. Is there a property right in information? Or is information something that should be free-flowing? And it can have practical effects, too. I mean, it's one thing for me to go on Amazon and look how they can tell what kind of book or record I would like, but also the collection of information about me helps, say in terms of credit, collection of information about my background helps others in terms of getting credit because that's what probability tables and things of that sort are put together with, to decide whether someone is a valid credit risk or not. You can tell by the length of years a person has held a job, or something of that sort and you can make predictions about their credit worthiness so they may be able to get a Visa card that's unsecured versus one that's secured, those kinds of things. So free-flow of information is important. Right up here. Can you say your name too?

RICH HELLER: Rich Heller from the Bill of Rights Institute and I bring everyone's attention to this article in the *Washington Post* of last Thursday at the Congressional hearing and Mr. Palafoutas, you hit it right on the head when you said the consumer or the user would like to know, and would like to have the option. This article says that we don't have full disclosure. This is the one where in the Congressional hearing one of the moderators told one of the Congressmen to click on a particular website and then when he reversed after he visited the website and then hit the backup key, he got an email and in his email was his complete mailing list, his telephone book, and a lot of other secret files like letters to his girlfriends or whatever that absolutely astounded him. He did not have the choice of even knowing what random websites would log in and just totally capture all the data on his desktop. Now, I don't think industry, from what I observe I don't see industry, giving itself any professional regulatory, any professional controls like that and it looks like, as much as I hate to say it, I don't see any option other than government, and I hate big government, the cancer government, like everyone else. What other options are there?

***The example you're talking about was a privacy caucus demonstration on the Senate side a few weeks ago and Christine Varney was there and pointed out that the "web bug" that you're describing violates the Electronic Communications Privacy Act. There are no known examples of that "web bug" being in use. It was a demonstration created by a group of privacy advocates to show what could be done and it was displayed and reported widely as if it's being done. It's illegal for that kind of "web bug" to be used and there was a little misunderstanding actually at the actual demonstration. Christine Varney was under the impression that they had found an example on the public Internet of this being used and she said, "I know that the Federal Trade Commission, or Justice Department, one of the two, let's get this site. Let's take this down right now. In fact, it's a demonstration of a possibility right now that kind of technology isn't in use though it's a security issue that's important to consider and there was lots of discussion that day about what's going on in terms of security.

***This is kind of kind of an interesting example. If I could take it one step farther. A lot of the press stories that industry is responding to, there used to be what I would call the privacy Edsel, you know, somebody had a neat idea for functionality, you know, we'll take this piece of information and we'll personalize it with that and we'll provide somebody with some customized

content. It got out in the press and it usually had the worst possible spin to it and it was an Edsel and the marketplace responded. The particular instance that you're describing I'd describe as a privacy phantom and there are other examples. I argue I'd say even the Toysmart case, the sale of the, the so-called sale of consumer lists in bankruptcy. It's an example of privacy advocates claiming that something that might happen or could be done, speculating about that but not talking about something that actually going on, that's actually occurring but kind of speculating that something in life happened and then reacting to that. Well, that particular instance was an example of a privacy phantom and as Jim mentioned it's something that Christine Varney, right there said, "This is illegal right now." What more can we, what more can industry do in terms of responding to that if it's not being done and it's already illegal.

CREWS: Right here at the back.

GARY LADEN: I'm Gary Laden with BBB Online Privacy Program and there were two issues that I didn't here panel address. Mark spoke about privacy, enhancing technology and John spoke about the regulatory climate, but I didn't hear anything about self-regulation and what, I mean we run a self-regulation program, there are others than run a self-regulation program. Beyond that, I also didn't here anything about the global context of online privacy. I mean, online privacy is not domestic issue in the borderless Internet. You've got the EU Directive, you've got laws being passed in Asia and Latin America. How do we deal with that?

***Well, let me address what—we're partners with BBB Online, so don't give me any trouble here, fella. Our third bullet in our press release is leverage market solutions. We think it's extremely important and as I think, Mark said, or I forgot what I talked about, the FTC did a report that said that, what is it, 98 percent of the most heavily trafficked sites has some kind of policy, privacy policy to protect. I don't think those are the problems. I think that people look at some of these other gangsters out there that may be out there that we get afraid of and I think we use those as the model but that's what's going to make the front page of the press, you know. When somebody goes to a regular website and one of these 98 percent websites, it's not going to be a story. The horror shows are going to go on elsewhere but I think the self-regulation is extremely important. What people forget is, it's worked. I think self-regulation has worked wonderfully. BBB Online was a trustee, some of the other programs are pretty good. Internationally we just haven't, that is real big, and there are problems out there, we need another forum on that because that's an even bigger issue and I think that's why it is. I'm just afraid to start dealing with it because it gets too big.

***Self-regulation has a very fox-guarding-the-henhouse connotation to it and I tend to describe the method of regulation that is the most free-market as market-regulation because its really about consumers regulating what privacy policies are available, or what the terms of those privacy policies are. Basically by absenting themselves from the marketplace, if the privacy offering aren't there, and I encourage, I'm absolutely as pro-Internet as you can get, but I absolutely encourage people to not use the Internet if they're not comfortable with it. Avoid the businesses that they're not comfortable with. That's market regulation, and I think BBB Online is a part of that process, but I think it's much better regarded as consumers regulating businesses than businesses regulating themselves.

***I would agree with that one.

DEANNE DEVIS: Deanne Devis with United Press International. It's been clear from the spate of federal and state regulation that there is a fundamental disconnect between industry and the consumers. Consumers basically don't industry and I'd like to know how you would address that. The issue of privacy policies that are not enforced, the issue of things when people do not know what is going on, not the least of which is the information that has been gathered without their knowledge up to now. There is a fundamental problem. Self-enforcement is fine if people behave themselves and behave as they, you know, say they will. But that isn't the question. The 98 percent isn't the question. It's the other two percent and it's not a fantasy with Double-Click and what they were planning to do with data mining that was something that was in the offing. How do your organizations look to address that very basic issue that there is no trust and you know, the idea of self-regulation? Yes, it does have fox-guarding-the-henhouse sort of feel to it.

***Well, if I could, I mean, one of the premises I would kind of push back on is the notion that there is no trust. The figures of the growth of e-commerce indicates that consumers are developing trust. It's happening faster, it's taking time, it's happening at different rates but certainly the growth is people are becoming more comfortable but it's a process of them becoming more comfortable but it's a process of their becoming more comfortable. We mentioned before BBB Online as being one of the tools of consumers have of feeling more at ease as they go to particular sites. One of the tests in all of this is whether or not there is supportive legislation, whether or not there is, in fact, a market failure. BBB rather, the Double-Click is an interesting example in that the FTC nexus for conducting an investigation of Double-Click was their voluntarily posted privacy policy. The FTC concluded after an investigation that they had, in fact, abided by the policy that they had posted. There wouldn't have been, I mean the process is one that takes time and develops as part of consumers but I think we should not confuse the public opinion polls about privacy. Are you concerned about privacy? It's a little are you concerned about happiness? We should not confuse that with a general lack of distrust on the part of consumers for the Internet because the figures are just the opposite.

***I don't mean to be argumentative, but Forrester Research indicates that, you know, hundreds of millions are being lost. The statement at the beginning of the panel indicated that people back-up and back away from commerce. You've got laws popping up like mushrooms in the early Spring. It's, with all due respect, it seems to have a very real monetary, fiscal right-now impact.

***Yeah, but the people who are affected most are the businesses and that's why they've got to do more of what Jim talked about in terms of educating the businesses but to say that people don't trust business does not mean that therefore trust government. I mean, it's sort of like, oh yeah, the government will take care of this. I mean, the worst line in the world from Washington: "I'm hear to help you." The other issue is what's being protected? I think there's, I think Mark used a great term, a "sense of creepiness" about this. Why am I apprehensive about Safeway? But you know, I am. It's emotional, I'm nuts, okay, I admit it. And I think some people have that same response to a lot of things that are going on in the marketplace because it's going on to fast. But the question that the press has to answer, and a lot of other people have answer, is what harm has been done? So what if Safeway takes my applesauce consumption and

sells it to somebody? I'm going to get some coupons, I guess. Now, the issue is to take care of some of the really bad stuff. I mean, Mark hit it on. There's sort of this anticipation that something really bad is going to go on. Identity theft is against the law. The bad guys are breaking the law all the time. You're not going to make this a risk-free universe. I think we have to deal with that. Now, when we have a real problem out there other than a hypothetical problem, I think that's what we've got to go into right now. But I think you've hit on something, though, the knife is to the throat of businesses to get consumer confidence up. And I think business is doing a better and better job every year. The Privacy Leadership Institute, some of the other groups that are working together are trying to do this but I'm not sure, well, I am sure, the heavy arm of government is not going to come and clear this thing up and you know, the fog will disappear and there will be a new dawn. I think we have to get the context for this. Plus, who is it, Lily, who put the recent, Lily or Pew Foundation, who had the recent, who was it? Pew Foundation, you know, they answer the question, do you have confidence, too, in business? Not too high. Who should make the rules, though? Half the people said we should make the rules, the consumers. I think we have to open that to more and more consumers, as both Mark and Jim said.

***A point that John referred to was the question of harm and I think that's one of the biggest questions in the privacy debate. In my study of the issue, I am seeing many threats to privacy coming from government and coming from the private sector; threats to privacy. Actual instances of harm, as legally recognized at any point, are fairly rare. I think people in Washington are particularly ignoring the fact that today, in every state in the United States, you can sue somebody who invades your privacy under the law of torts, there's a privacy tort, embarrassing disclosure of private facts, is a tortious breach and are those suits happening to some extent, we're testing the waters as far as what happens in the online environment, but the right to sue is out there and it should give some people assurance that there are limitations to what can be done with information.

CREWS: There's no question that mistakes are going to be made as we go along, but some of the biggest customers now for privacy software and privacy options are big businesses who have to assure the confidentiality for their kids or new options for American Express for random credit card number generation and even cards that you use by pre-paying so that you can go online and purchase things without revealing your identity at all. And plus on the opt-in issue you debate opt-in versus opt-out, but in a lot of ways those decisions are getting made in the marketplace. The wireless web, which is virtually non-existent, but presumably that's where we are heading, a lot of the companies who are in the business of trying to make that happen are adopting opt-in alternatives on their own because one of the issues you'd often hear about that you'll be buzzed as you go past Starbucks or McDonalds that they have a discount for you in there. But companies who are going to be offering those services are beginning to embrace opt-in of their own accord. We had a question right here at the front. Can we get a microphone right here?

SUZANNAH THOCKS: Thanks, my name is Suzannah Thocks. I'm with the Pew Internet and American Life Project. Thanks for citing our research, and indeed people did find in our survey that they have that creepy feeling, but they are no less interested in using their credit card online than they are to use it over the phone. But again, what we also found is that only a third of people knew what a cookie is, only 10 percent block it, so although they have that creepy feeling

and they're using their credit card, they're making friends, they're using dating sites and all sorts of other social high-trust activities. What about the fact that people don't know what's going on, and I'd love to hear from the two folks who didn't talk. I know Mr. Harper spoke about that but I'd love to hear what...

CREWS: What's the question?

THOCKS: About consumer education. What industry needs to do about consumer education.

***Well, we've got to be more aggressive, but on the other hand, it would be interesting to find out how many people, and I won't ask the question, but in your own hearts answer it. How many of you have conducted a transaction on the Internet? Bought flowers, or bought, you know, something from buy.com. I'd betcha there'd be a lot of people in here. How many click the privacy button? I'd betcha very few of you did. I've never read a privacy statement other than to go to somebody and get some shots in about their privacy thing. That's the only thing. Jim's hit on it. Consumers have to do a lot, but businesses have to be more aggressive, and they're being more aggressive to get that confidence level up. I mean, look what's going on with credit cards now. I mean, I think American Express was one of the first ones out. It came out with an ability to use a credit card number on the Internet that was different from your other number. Now you've got disposable credit card numbers. I mean the market is responding and I think it has to be more aggressive, especially as the economy is turning down a bit, or flattening out. I mean businesses are going to have to be more aggressive on this and they are.

***I'll chime in that this is also very much a generational problem. Those of us fuddy-duddies, in our early thirties don't understand what's going on and the people who are 12 and 13 are laughing at us, they're probably watching us on steaming video right now and just snickering. But this is a problem that will have an S over 10 or 15 years completely, if nobody takes particular extra efforts, now, where we demand everything right now. So aggressive efforts by industry, maybe efforts by government to educate consumers and truly empower them are the way to go.

***It's obviously a real challenge in our technological age for consumers to understand, you know, how a car works and kind of the ins and outs of a lot of things that we use. But I think they understand a lot more than perhaps what we're giving them credit. Clearly there is this phenomenon that people are reluctant to give information when they're online unless there's a description of kind of a value proposition. We want this information because we want this information because we want to send you coupons or we want to give you some additional benefit and I think most sites will find that if they simply put up, you know fill out the box without any kind of benefit there they won't get the response rate that they will when they explain what it is they do. And of course because of privacy policy and the Unfair Trade Practice, legal consequences that require them to do that. So while, I mean I agree that, you know, cookies is one of those issues that bubbles up and down and it sounds ominous and then it kind of recedes and then it comes back again. People know about as much as they want to know and they care about and there's also a range of interests that some people care very, very deeply about privacy and they are those privacy fundamentalists at the polls show about. And there are other people who are candidly less concerned and not as worried about the information and more

willing to share information and exchange information and feel quite comfortable and don't need to know a lot of stuff about this.

CREWS: If you all would thank all of our speakers and we'll have lunch upstairs.