Law, Policy, and the Convergence of Telecommunications and Computing Technologies

March 7-9, 2001

PERSONAL PRIVACY IN A CONNECTED WORLD

March 8, 2001

DEAN JEFFREY S. LEHMAN: . . . . Two in the morning and then a lunch speaker and then another panel this afternoon. I'd like to, without further ado turn the microphone over to the Dean of our School of Information, John King, who will be the moderator for the first panel this morning. One of the great things about technology is that we can't do a thing about the fact that there's a light switch at the back of the room right where people are inclined to stand and lean. And yes, that's the head of Information Technology at the law school who, in fact, leaned against the light switch and is turning several shades of crimson this morning. Okay, here's John King.

JOHN KING: Thank you very much. If our panel could come to the foreground we could really get going here. While they're getting seated I'll just make a few introductory remarks. I am John King. I am the Dean of the School of Information here at the University of Michigan. Welcome, thank you for coming out. This is very exciting. I can tell you all that you should take advantage of minor technology marvel. Yesterday I was tied up in many things but I just could not miss the keynote address. So I looked at it on the webcast and the quality was very high. There's a website you can go to if you can get it from the law website here if you're missing any of these events and just click on the webcast links and you'll be able to see this entire affair which is really very exciting.

Okay, before we do the introductions I just want to give you a couple of protocol observations. We're going to run this fairly tight schedule because we do have constrained time so I'm going to ask the Attorney General to speak for 30 minutes and the panelists for 10 minutes each. We've got a little wiggle room there but not a lot. I'll be tough and hold them to it because we need some time for the questions. That's a crucial part of this enterprise. The protocol for questions is to write them down, there will be some cards passed out. You simply hand your card to them and they come up here and we take the questions from the cards. There's also a yellow sheet for you for this panel. As the question session is going, if you would write down on this yellow sheet what you think crucial questions are and turn them in on the tables out in back afterwards. This is going to be a very important part of the product of the conference because we're going to try and synthesize the key observations, insights that arise out of this open questions, if you will, remaining to be settled.

Okay, without further ado, I'd like to introduce our panelists. Our key speaker is Attorney General Jennifer Granholm. She's a Phi Beta Kappa graduate of the University of California, Berkeley and an honors graduate of the Harvard Law School. She clerked in the sixth circuit and became head of Wayne County's law department in 1994. In 1998 she was elected Attorney General of the state of Michigan, and she's focused her prosecutorial sights on child and senior citizen's rights and consumer and environmental protection. As Attorney General, she has

introduced a new high-tech crime unit, which has enabled her office to be the nation's first to bring criminal charges against a company selling illegal drugs using the Internet. As a result of this, her office has become a resource for law enforcement agencies seeking to learn more about Internet crimes.

Our first panelist is Jeffrey Rosen, an associate professor at George Washington University Law School where he teaches Constitutional Law, Criminal Procedure and the Law of Privacy, and he's author of a book called *The Unwanted Gaze: The Destruction of Privacy in America*. And our other panelist is Jonah Seiger, co-founder and chief strategist of mindshare Internet Campaigns, a leading online political strategies firm in Washington. The firm helps issue coalitions, non-profit organizations, corporations and trade associations use the Internet for political organizing, outreach and advocacy.

ATTORNEY GENERAL JENNIFER M. GRANHOLM: Well, I appreciate the invitation, Dean Lehman to come here because this is an area that my office has been operating in and going where no man has gone before and so I really enjoy the topic and I love the fact that, of course, the University of Michigan here is on the cutting edge, as usual, and we like to think that our office is on the cutting edge. The notion of converging academia and government and business is a great concept in the new economy because we've got to borrow from one another. We've got to link; we have to forge unusual partnerships to be able to address some of these issues. So, glad to be here.

Now as my hat is a pragmatic one, being the Attorney General of the state of Michigan and I love to steal as much as I can from academia, I look forward to seeing the results of this conference. And hopefully we'll be able to borrow some for even our Lansing legislature if such results come about. Well, let me say first of all that privacy is really not my favorite subject. And for folks that followed a lot of the actions that we've taken in this realm, it may be difficult to believe because we really have been on the forefront in our office in going after the privacy rights of individuals on line. Medical privacy in addition to that which I'll talk more about in a minute.

But, in reality privacy is not my favorite subject because I don't think in the bigger scheme of things that's really what we should be talking about. I don't know if any of you know Robert Putnam's book Bowling Alone. It's a great book I was introduced to not long ago, and I think about it every time we talk about privacy in my office. And if you haven't read it, Putnam argues that we are suffering from a serious diminution in civic culture in our society, or civic engagement with one another, our need and our propensity to connect with other human beings as some sort of community is suffering. Even if it's as small a community as a bowling league it's dwindling rapidly. Forget about civic involvement in terms of the voting rate, which is sickeningly low. Just look at the trust rate, which is also alarmingly low. Social networks are deteriorating, we are a society now of leaders and of consultants, certainly consultants and of managers, but not of joiners. The percent of people who now attend any public meeting continues to fall. There's a 50 percent drop in the last 25 years. My guess is folks in this room wouldn't be here were it not related to your job in some way. So the question really is what's to blame for that loss of togetherness, this surreptitious unraveling of the social fabric, the

community. And I think there are lots of things. We're mobile, we have much less free time, there's no war, there's no depression to force us to bond together. There's no rich, collective experience anymore. Technology certainly has made our lives so much more convenient and efficient and it's certainly played some role in that isolation of society. So what I really care about, what I really care about as Attorney General is to find out if there are ways to promote social and civic interaction and community engagement. That's what I love to talk about. But what I'm asked to talk about more often is privacy. And so I have a different spin on this issue. Are the two connected? I think that they really are and I think it depends on how you define privacy.

Jim Tierney, who's the former Attorney General of Maine, and I talk about this all the time. He's a real privacy guy as well. If you believe the most extreme privacy advocates one would think that privacy is all about being left alone. You're sort of reminded of Ebenezer Scrooge in Dickens' *A Christmas Carol*. The extreme privacy advocates, no one here, the extreme ones want nobody in their lives, they don't want anybody knocking on the door, they don't want anybody coming to collect for the poor, they don't want anybody, no nephew inviting them anyplace. They're so concerned about privacy, and their rage often is so intense that they don't care about any of the good things about interaction. When they talk about business, the extreme folks, they neglect to mention that there are some positive sides of marketing, positive sides of a customized Internet experience. When they talk about their real opponent, which of course is government, they seem not to care about deadbeat dads and the collection of child support or Medicaid and insurance fraud, or tracking child molesters, or sexual harassment in the work place. The extreme privacy zealots seem kind of joyless. They don't want to use a debit card at the grocery store. They want to pay cash to avoid leaving a trail. They'd rather die than buy a pair of pants at EddieBauer.com and for the true privacy diehards, therefore, it is all about separation and about not coming together. So if being a privacy advocate means being left alone completely, I am no privacy advocate.

But what if privacy really means something else? What if it means, just a different spin, what if it means for the ability for us and for the private sector to create a safe space. Turn again to fiction and It's a Wonderful Life, one of my favorites. George Bailey, Jimmy Stewart, in most ways he is the least private guy in the world. Everybody knows everything about him and his family. He runs a bank; he knows how much his neighbors have in the bank. He worries about them so much that he can't even sleep at night. George Bailey makes the world better. He's our hero. He lives in a safe and connected place, in Bellows Falls, Vermont, where the grocery clerks say, "Morning, George" and the police officers are named Bert and Ernie. Now, what's that got to do with privacy? I think it's got a lot to do. If the goal is to create a safe place. Now what I'm talking about is not a place of isolation but a place where we can be open with ourselves. Where we can have trust in the companies with which we do business. Then privacy, therefore, is a good thing. This is a market response. Companies who deal online need to create an environment where people trust the online world, where they trust the ability of giving their information away. The safe spaces, of course, can be geographical, can be bricks and mortar spaces, like doctors offices or insurance companies, and they can be cyber communities like an online mall or a medical information site. But they've got to be safe. They've got to enable people to trust them. So when anyone uses personal information to destroy our ability to live in a safe place, then I care a great deal about privacy protections. So where does this go? This is where, as my grandmother used to

say, this is where the cheese gets more binding. Don't ask what that means but it's a really great line, don't you think?

On the one hand, the Internet is a relatively easy thing in terms of law enforcement and government regulation at least as I see it. We set up a high-tech crime unit, as was mentioned, a year ago to make the online world a safe place for kids in particular. And in terms of businesses, especially in terms of consumer issues, the Internet cannot be known as an enforcement-free zone where any new economy business can go and avoid the law to get a foothold, a competitive foothold, over their competitors by fraudulently or deceptive advertising or luring people in. And of course it goes without saying that purely criminal activities like child pornography online and drug sales on line or criminal wherever they occur whether it's in the bricks and mortar world or on a website. But in terms of privacy, in terms of privacy, well it may not be spelled out explicitly, I think the right of privacy, I know it's been discussed in more than 700 Supreme Court opinions and countless lower court decisions across the country. As many of you may know the Supreme Court has concluded already in several cases that the concept of privacy is already imbedded in the fine mesh that is the Constitution and the Bill of Rights from *Lloyd vs. U.S.* in 1894 where Justice Harlan in 1894 wrote that "of all the rights of the citizen few are of greater importance or more essential to his peace and happiness than the right to personal security." In 1946 Justice Douglas in Griswold vs. Connecticut writes, "we deal with the right of privacy older than the Bill of Rights, older than our political parties, older than our school system. Privacy has been part of the legal landscape of our country for over a century."

So the question of protecting that penumbra of a right in the face of technological change is what's upon us. Change that's not envisioned by Justice Douglas in the '40s, certainly not by Justice Harlan two centuries, at least in 1894. So as the technology evolves so has got, the common law has to evolve as well. And notice I didn't say regulating. The common law I believe has to evolve. I think there are some areas, areas where people cannot protect themselves, where they don't know how to protect themselves, where newer expanded law or regulation law has got to be part of the answer. Child protection, the children's online privacy protection act etc. puts the onus on websites and tech companies to help protect children because children cannot be expected to know what is going to happen to their information and be able to protect themselves. Financial information, insurance information, when we give that kind of information over to a bank or an insurer. That information certainly ought to be protected by law. Medical records should absolutely be protected from invasions of privacy. When you entrust that information to a health care provider any health care provider whether it's your doctor, your dentist, your pharmacist, or your optometrist, whatever, that information should not be sold off or disclosed to a third party without your permission. Last month in Michigan we introduced a bill that would provide a framework, language framework, for protection of one's medical privacy rights here. And Michigan's hot topic.

But in terms of privacy generally, what is and what can be the legal baseline? Where do we go? Where is the place where government's role is not too hot not too cold but just right? Where creativity blossoms and yet no one is harmed? There's never a perfect solution, but I have run the gamut in my thinking on this from a perspective that would insist, when I first got into this, on a strict opt-in basis to a perspective now where I think we've got to set forth a basic privacy right, which is articulated in law, for sensitive, personally identifiable information and allow the market in its creativity to respond to that right. By the time the government starts getting around

to regulating ISPs (Internet Service Providers) or regulating at the level of code, or regulating the browsers, or regulating the language in a privacy policy, Moore's Law has rendered the regulation obsolete. So I don't want to be talking about the technology. That's the business of many of those who are in this room. What I want to talk about is the law that the technology may respond to. So I prefer a basic right that rings true in the online world and the bricks and mortar world and that's where we started with our medical privacy bill and that's where I think we've got to be headed.

The National Association for Attorneys General, acronym NAAG, is working on, has issued some privacy principles. Many of you are aware of the basic privacy principles that many people have talked about the fair information practices, principles, notice, access, correction, opt-in for sensitive information, opt-out for non-sensitive PII (Personally Identifiable Information), those are the basics of what the NAAG principles have offered. Those are good but they really beg the question. The question is what is the legal right that those principles are seeking to protect? What is it that's articulated in law that those principles seek to protect?

When I first started looking at this. In fact, in January of last year there was a conference at Stanford where all of the attorneys general met and we began to explore this issue of privacy, especially in light of the technology. And many of us started out with the notion that personal information, data collection, should be a property right. And that property right the individual can negotiate away with a website in exchange for a discount. But the problem with the property right is that as all property rights, it's alienable. And so once it's gone, it's gone. It's sold off continued down the line. It's the same problem I have with these medical waiver, the release forms for medical records. Once you sign this blanket release it's gone. You can't get it back. You can't be an Indian giver with respect to your own sensitive information, your own data stream, your click stream. So privacy as a property right, I have a problem with that.

But what if, what if we took a look at the torts. Now as an attorney general I run the largest defense law firm in the state so I'm not real excited about expanding torts, however, it's going to happen. One way or another we're going to see privacy protected. And I really think a tort-based invasion of privacy spectrum where somebody's personal information cannot be released if it brings somebody harm might just be the way to go. Let me just expand on this a little bit.

Justices Warren and Brandeis in 1890 gave us the original notions of a right of privacy tort in a Harvard Law Review article. And those original torts, which still exist in the common law, the invasion of privacy torts they are as old as the hills. You know they talk about intrusion into seclusion, they talk about appropriation of an image, they talk about publication of private facts, they talk about false light and you know any of you who are lawyers and have gotten Prosser's book on torts you know it's all in there. And all of the states have some judicially recognized or statutorily created right of privacy of those kinds of torts. What I'm proposing is a refinement of those for the release of personal information. So clarifying or evolving that existing privacy tort makes sense to me in the common law for a number of reasons. One, the courts can be much better suited to carve an issue with a scalpel and not with an axe on an individual basis to determining what constitutes a particular privacy offense. They might be better than an elected body that is often subject to background noise of lobbyists and election campaigns and interest groups. Courts might be in the best place and they have the ability, courts do, of being more fluid than either legislative or a regulatory response. The courts are, it's their job to be well adapted to

balancing the reasonable expectations, in this case the reasonable expectations of privacy and society's expectations as technology changes. So this is what I'm thinking of. Clearly there are limitations to a right of privacy that people willingly give up by living in society. Do you have the right to expect that your phone number is going to be kept private when you've allowed it to be published in the phone book? Obviously not. Where do you draw the line? So the courts have got to fashion, or the legislature can fashion, an appropriate standard to govern the ability of someone to bring a tort action under a right of privacy, an invasion of privacy, tort. And legally for purposes of a personal information tort remedy, I think there needs to be sort of four threshold questions that would need to be asked.

One, the person who's bringing the action has to have a reasonable expectation of privacy, that's clear and we can talk about how that's evolved through the law over the course of time. The second, the basis of the transfer of the information, the personal information, in order to bring an action, I think has to be for commercial purposes. You're not going to bring an action because somebody transferred your Christmas list as long as it's not for commercial purposes. Three, the information has to not be a matter of legitimate public concern. And four, the invasion of privacy has got to be serious enough to warrant judicial intervention. These are all subject to a court's determination on a case by case basis. But it's a reasonable threshold. The biggest question is what is a reasonable expectation of privacy? The right of privacy, like all other rights, should be a culmination of what society deems socially important enough to protect against abuses. The law should seek to redress the invasion of the sanctity of a person's dignity or right of privacy, but people should expect some loss of privacy as they interact with the world around them. So in the context of the Internet, businesses obviously need a base level of information about the people they are interacting with. The consumer who's shopping at an online retailer should expect that if she makes a purchase that information is going to be conveyed to a shipper like UPS (United Parcel Service) who's going to deliver the item to your home. That's a reasonable expectation about where these transactions would go. Without any information telling her otherwise though, that same consumer does not have a reasonable expectation that her home address is going to be shared with another party. Or potentially her shopping preferences are going to be shared with another party that has not been, that she's not been told about.

In Michigan we don't have a good law yet that protects people's information or click stream. So we have taken action under the Michigan Consumer Protection Act, and this is not a tort, but we have taken action against DoubleClick and sites like Procrit.com and Itsmybody.com and Stockpoint.com and Ifriends.com, one is a porn website, one is a medical website, one is a website directed at adolescent girls, DoubleClick most people know about. The point we were making is that people who interact with these websites were not being told that third parties were on the website tracking. And all I'm saying is that in a proposed tort scenario a person does have a reasonable expectation of privacy unless the website does something to defeat that reasonable expectation of privacy like a well-articulated, visible privacy policy which lets people know. That's just an example but the technology can respond. You have a box that pops up, how do you let people know that their information may be tracked? The problem is now people get onto websites and before they even have a chance to checkout the privacy policy, whether the privacy policy tells you it up front or not that they're being tracked by third parties, but before the consumer receives any information they're already tagged with tracking technology, whether it's a web bug, whether a third party cookie, whatever it is. Therefore the websites, the companies have a tremendous advantage over your average Internet user who doesn't know what the heck is

going on. And surveys show that even the more frequent users, the more sophisticated users of the technology still are not aware, fully, of what is going on. Many people, you know this, most people when they pull their computers out of the box they have no idea where the defaults are set. They have no idea that automatically the cookies are being attached. And the market has not responded effectively, I think, to combating the placement of third-party cookies. I think that people should have a choice about that. About turning off third-party cookies, leaving first-party cookies, I think the defaults should be set differently, but those are technological issues. I think consumers need to be informed but they do have a reasonable expectation of privacy and it's up to the technology to respond and figure out if they're going to defeat that reasonable expectation of privacy, how they do it. Whether it's a well-publicized privacy policy, whether it's some other means, they can defeat that threshold question but the technology needs to respond. And if they fail to defeat the expectation, then a consumer might be able to bring an action under the theory that I'm proposing.

A couple of other sort of threshold limitations that might need to happen in terms of the purpose of the transfer of information. Obviously a tort would not be allowed to prevent me from sharing as I mentioned the names of my Christmas card list with my brother in Vancouver. The tort is intended to prevent companies from profiting off the sale of personally identifiable information without the consent of the person being identified without their expectation. When they've defeated their expectation of privacy, when they haven't defeated it. Similarly, if the information is not, if the information is newsgathering information, has a legitimate public concern that would defeat a privacy scheme because there is a legitimate public concern. For example as personal as the development of a contagious disease is, there are certainly legitimate reasons to inform the public to prevent the spread of the disease, the news gathering function I think would be exempt under that kind of prong.

And fourth, the fourth sort of threshold question that would need to be answered before a successful invasion of privacy tort might be allowed is as with other torts there has got to be some element of intent and it's not just mere negligence in order to trigger it. It's got to be a serious breach. Those are issues that a court can look at. Is it less serious, a court may differ on this but somebody might say that the sale of non-PII in bulk to be able to target ads is a less serious breach certainly than the sale of somebody's home address, the sharing of data about visiting a medical website, etc. Those are all in the spectrum we're all familiar with the spectrum and a court might be able to look at that and draw some lines. So the bottom line for me is something's going to happen. You have seen all of this activity in Washington. Everybody is moving down this path. The question is who is going to win? Which lobbying arm is going to be stronger? Perhaps a safer route would be to allow the judicial branch to weigh in on this without crushing the creativity of the economy and allowing a case by case intervention.

In 1890 Warren and Brandeis they were responding to the camera, which was the newfangled innovation at the time that all of their privacy concerns were centered around that piece of technology. And today of course we have the 'net. But in 1890 they wrote, and it's true today, "the individual shall have the full protection in person and in property. That the individual will have this is the principle as old as the common law. But it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social and economic changes entail the recognition of new rights and the common law in its eternal youth grows to meet the demands of society."

So what makes this whole realm so great is that we are, we're on the front, this is one of the chapters that's still waiting to be written, which is why this kind of conference is tremendous. We're still standing at the beginning holding the pen writing the new words instead of being on the back side flipping back to erase or to rewrite or to recalibrate. It's our chance to forge a new partnership, to get some different kinds of views out there, to change the minds of and the perspectives of those who might be regulating, of those who might be making rules here that are set in stone that we don't want to hinder creativity down the road. But it's the best time, too, to create a safe place, a trusted space for consumers to go without them feeling like they are going to be taken advantage of and their information sold off to the highest bidder without their permission. We need to create a place where people can comfortably go online and interact. Jeffrey, you wrote in your great Eroded Self article that, I don't mean to steal your quote if you're going to give it, but it's such a great quote. "There's nothing inevitable about the erosion of privacy in cyberspace just as there is nothing inevitable about its reconstruction." I know there was a famous quote from the CEO of Sun Microsystems that, "There is no privacy get over it." That's not the kind of world that I think any of us want to live in. And so we can reconstruct it. We do have the ability to rebuild some of those private spaces that we've lost. And all we need, as Jeff Rosen says, is the will. So hopefully a conference like this will demonstrate that we have the will and the ability to balance both sides. Thank you.

JOHN KING: Well I can't help but make a little bit of a segue with an anecdote. One of my doctoral students, Laship Halen, when I was at the University of California at Irvine did her doctoral dissertation on the setting of defaults and shared calendar systems as they are shipped by the manufacturer and her research site was Sun. And on all the Sun Microsystems products that are shipped that contain a shareable calendar infrastructure the defaults are set for universal read access to everybody's calendar. But when you go to Sun and try to get to Scott McNealy's calendar that default has been changed and apparently he hasn't gotten over it. Okay, we're going to turn now to Mr. Seiger. He's going to follow with his comments.

JONAH SEIGER: Thanks, John and good morning everyone. When I was a student here, an undergrad at the University of Michigan I made a policy to never have a class before 11 a.m. so this is a new experience for me to be in a classroom at a quarter to 10.

Thank you Dean Lehman and all of you who organized this for inviting me to be here today. It's a great privilege. It's also a great privilege to be able to follow the Attorney General who's been a tremendous leader in the field of privacy and has really done tremendous work in raising the profile of this issue here in Michigan and putting pressure on the folks I work with in Washington to do the right thing.

I come at this with a sort of a unique perspective. I have a foot in a lot of different worlds in the privacy debate. As John mentioned in his introduction I am the co-founder and chief strategist of mindshare Internet Campaigns. We're an online public affairs consulting firm that develops Internet communications strategies for issue advocacy organizations. A number of my clients are

Internet policy organizations that are working on the issues of privacy. I started my career working on Capitol Hill working for Congressman Ed Markey who is, as many of you know, a leader on the privacy issues. And then from there went to work for a couple of public interest groups including the Center for Democracy and Technology, which I helped to start and which has been a very aggressive advocate of privacy. And in my current life as essentially a media consultant that develops Internet campaigns, we are in the business of, on behalf of our clients, building and maintaining constituencies, which includes the collection of personally identifiable information. So from a very real basic perspective I touch this issue every day both from a practitioners role but also from the standpoint of the policy debate to which I have a front row seat.

I think, just as the Attorney General talked about, definitions of privacy are very important. I'd like to just follow on some of the points that she made there. Our case law and our constitution talks about privacy as a right to be left alone, or has been interpreted that way and it's been applied mostly in terms of electronic surveillance. And the rights of citizens with respect to government access to their private communications. And there's a very rich protection under the fourth amendment. Battles are constantly fought there. I spent a number of years fighting the government's attempts to create guaranteed access to encryption. Some of you have probably heard about the key escrow and the clipper chip and those issues. But in the area of data privacy it's a lot more muddled, the state of law and expectations. And we have sort of different expectations for financial information and medical information.

In my mind the definition of privacy that's relevant to this discussion is a question of control. And I think that we, the Attorney General and I, would agree that the core issue is that consumers should have control over how their identities are managed online. I mean that's a fundamental point and I think that it underlines the entire debate over this issue and I think it's a very basic principle on which we can all agree. And that this can be accomplished through a combination of technology and law. But at the end of the day it's about giving users, individual consumers and users, control. To empower them to take control over their identities.

The issues that are raised at the federal level here come down to how do we provide that control to consumers? The Attorney General talked a little bit about the NAAG, the National Association of Attorneys General, principles. And this has caused quite a stir in Washington as the Internet industry tries to come to terms with how privacy might be regulated. And there are a couple of key issues that I want to dive into in little more detail.

The first goes to and in response to the comment about a judicial approach to protecting privacy, is the issue of federal preemption. If states are enabled to develop different standards to treat personally identifiable or even non-personally identifiable information differently, then we're going to have a really hard time doing business on the Internet nationally. Not to even talk about the global challenges there and we've already run into this with the European Union. But if we have 50 different state standards for privacy, it's going to be extremely difficult for anybody to do business in this medium. And so while I think it's appropriate for states to have a significant role in enforcement of privacy laws and to give deference to states in that area, it's also, I think, one of the core issues that we're going to have to confront if we're ever going to have a federal privacy standard, and I would posit that if we believe that a federal privacy standard is necessary then we must address the balance of state preemption.

Bill Lockyer, the Attorney General of California, who's been leading the National Association of Attorneys General draft principles process, has compared the state's rights in this area to their rights to set clean air standards. Now I think that states should have a very important role in setting clean air standards. If you're living in California and there's a smokestack in California that's going to affect you much more than the smokestack in Nevada. But when it comes to a medium that really knows no borders, where you can be doing business from Washington, D.C. on a server in Seattle and in San Francisco simultaneously, it gets very hard to understand how to actually in practice respond to differing standards for privacy. So I think it's fair to say that as we look out at the legislative landscape in Washington that the big issue we need to confront is the question of federal preemption.

Another issue that's very important when we get into this understanding of privacy as being control or consumer choice is what exactly does choice mean? The Attorney General talked about third-party cookies and a concern that sites collect a cookie even in some cases before an individual can find a privacy policy. But there's a difference I think in kind between the collection and use of personally identifiable information and non-personally identifiable information. Setting a cookie on a website when you first visit that just identifies as a unique user but doesn't have any personally identifiable characteristics I think is a difference in kind than personally identifiable information like your name, your address, your email address etc. And in terms of giving control, there's a difference I think also in kind between opt-in and opt-out. The National Association of Attorneys General principles have two things that are real concerns to a lot of people in the industry. The first is as I mentioned the preemption issue. The second is that in effect many people read these draft principles to create a national opt-in standard. A requirement that in order to collect any sort of information sites would need to have people opt-in. That's a much more restrictive standard than exists today in the brick and mortar world. And in my mind is unnecessary for the basic non-personally identifiable information that's collected.

Looking at the state of play in Washington, we've spent the last couple of years working in the area of self-regulation. The industry has invested a great deal of energy in trying to develop practices for self-regulation and these have worked fairly well. According to a sweep of the FTC, The Federal Trade Commission did an analysis last year or actually now almost two years ago, in May of 1999. The top 100 sites on the net they found that 66 percent of them gave consumers notice. A privately funded study found that 95 percent of the top 100 sites had some form of privacy policy and that that was up from 71 percent in 1998. We don't have numbers for 2000, but I think that that's a positive trend.

Some of the groups that I represent, I should say the groups that I represent have a broad range on this issue and I want to make very clear that what I'm about to say is my own opinion and I'm not here to speak on behalf of any of my clients. But I think that we're ready now to have federal legislation establishing national standards for privacy. I think that in order to, as the Attorney General talked about, foster trust in the medium and continue the growth of this medium we need to establish some basic standards that consumers can rely on that their information is going to be protected and used. And I think that a reflection of the fair information practice enshrined in law makes some sense. Notice and disclosure: privacy policies need to be easy to find and say what a site is doing with information that they're collecting. Choice and consent: consumers, individuals must have choice regarding how information is collected and used. Data security: they should have confidence that the information that's collected is going to be secure. They should have an

assurance of the quality of the data and access to the data to change records and correct mistakes. And finally, I think another as I mentioned critical component is federal preemption. I think that we must have a uniform standard that enables states to enforce the laws but a general expectation for somebody doing business in the United States that they don't have to comply with as many as 50 different standards.

There are a bunch of bills that have been introduced in Congress that sort of cross the spectrum. There are the privacy extremists as the Attorney General mentioned who are seeking to create very restrictive standards. There are those who still argue for no legislation to let the industry self-regulation practices work. And then there are those like Senator McCain, Congressman Eshoo from California, Senator Wyden, Conrad Burns from Montana who are talking about legislation along the lines that I just discussed. And I think that in the next 12 months, once we get through the budget fight and probably campaign finance reform and the education bill that this issue is likely to be teed up. And I think it's fairly likely that some form of legislation stands a good chance of passing. But it's very important to understand that the balance of power in Washington is such that it's very easy, or I should say, it's easier to stop legislation than it is to pass legislation. A 50-50 split in the Senate and a six-vote majority in the House means that consensus is a vital component. And, again, these issues regarding opt-in, opt-out and preemption make for a very important place where consensus can be found. Again, just to sum up here, I think what the Attorney General has done, her leadership here in going after sites that are bad actors, in drawing attention to sites that aren't living up to the privacy policies that they post, is very important and plays a critical role in the enforcement of privacy rights and in pushing the issue along. But I think as we look forward to and understand how to best address these issues we need to be very careful about the distinction between opt-in ad opt-out and we also need to be very conscious of the need for a uniform national standard. Thank you very much and I look forward to your questions.

JOHN KING: The blue question cards are on their way to you now so you can start preparing them now. Mr. Rosen.

JEFFREY ROSEN: Declined to have his remarks published.

JOHN KING: Okay, I have seven questions and rather than go through them serially, I'm going to batch them and I've used my moderator's prerogative to cluster them in descending order of abstraction. Well it looks like I have eight now. I'll see if I can find where this one goes. Okay, I know where that goes.

There's two at the highest level. The first one is, is personal information so ephemeral that there would be an undue burden in proving a tort action? Could this problem be addressed through individual controls such as opt-in?

Another one is, with regard to the tort approach on privacy what about the death of a thousand cuts in which each individual's loss of privacy is too small to meet the threshold but the overall cost to society is large, who will file suit? So that's one question.

Second, there seems to be disagreement between those who believe current laws cannot be stretched to apply to the Internet and those who want to let the common law evolve. Do you believe that allowing the common law to reinterpret current laws is a wiser way of proceeding than new legislation? Would new legislation perhaps prove counterproductive? And in the same vein. Is it reasonable to expect that the current U.S. Supreme Court or a new court with George W. Bush appointees to further define, or permit courts to define, privacy rights in the absence of explicit new legislation, which may in turn thwart Internet development?

Okay, then in a different vein. If we have privacy policy on websites, won't the policies become so onerous that users will not take the time to read them? It's like any license agreement that users don't read but instead hastily click "I Agree" and move on.

Do you think privacy rights should limit law enforcement's use and exchange of personally identifiable information such as DNA databases? How would law protect the individual from use of information gathered by marketers, by the government, for instance to enforce the use tax in Michigan? There's one more here. How are local governments managing resident-based privacy issues? Information from transactional exchanges, what are the key issues for municipal privacy policies and can you recommend readings?

And the final one, which is explicitly intended for the Attorney General, what are your views on personal privacy for public officials?

ATTORNEY GENERAL JENNIFER M. GRANHOLM: Those are a lot of great questions. And let me just clump some responses and I'd love to hear from you in particular, Jeffrey, because I'm so intrigued by your great remarks. So profound and poetic and yet I still want to know what's the answer. As a pragmatist I want to know how to fix this problem. And I have, I have and I hate to say this as an elected person myself but I have just this great cynicism about the ability of a legislature to craft a solution that is effective. And that's really where I come down because of the influence of great organizations like yours who are pushing them; that's democracy at its greatest, you get lobbyists on one side and on another who are pushing. But I worry about things like the Gramm-Leach-Bliley Act passed last year, which I think did not provide the kind of protections that were needed basically because there was a very powerful lobbying group, the financial institutions, who were there on the federal level to prevent any curbing of their ability to share information and to gather it. And so they say, the Gramm-Leach-Bliley Act says we're going to, if you're a financial holding company you can share information, if you own as a holding company a bank or an insurance company or a mortgage company you can share all that data among yourselves without having to get the consent of those who are under your rubric, your customers etc. And if the states want to enact something greater, the legislatures of the states want to enact some greater protection, then let the states do it. Well, the reality is, every state that has tried to enact something in the wake of Gramm-Leach-Bliley has had a herd of lobbyists descend upon the state to prevent just that from happening. So I just

worry myself about the thresholds that federal legislation would be able to successfully enact and. therefore, that's why I was left with the courts. Now I'm intrigued by the political piece of it, Jeffrey, and the ability of consumers to rise up in outrage. I just worry, the average consumer is just not aware of what is going on and there may not collectively be enough will. There may be some sophisticated folks who are willing to stand up and say things but it gets tiring after a while to have to do it at every piece. Talk about a death by a thousand cuts, every time some invasion occurs if we are to rally and you know get people exercised about this and get the shareholders excited. That's a lot of effort unless you've got some recourse, some ability to go to some forum that will address your concerns. Which is why I ended up going the circular route back to the judiciary because I think that of all entities, and my cynicism hat is still on, but of all entities in the system the judiciary is arguably, should be anyway, the least biased and the most able to redress problems on an individual level. And yes there is the potential of a death by a thousand cuts on that, but, it's less, at least there's individual opportunity for redress and then the specter of law being made that is able to guide companies as they go forward. So I don't think there's a great solution anywhere but I do think there are possibilities in these different realms. And I just think there has to be some threshold articulated somewhere, which gives people some comfort that they are able to go online.

Who will file suit? This is why this issue of preemption is such a critical issue for the attorneys general. If an individual doesn't meet a particular threshold, the Attorneys General should have the ability to go forward and enforce and potentially argue that their state law should be raised to a different level than perhaps what was in the federal law. I just don't like these hybrids that we are seeing in the wake of Gramm-Leach-Bliley because there's nothing that is happening on the state side that is able to follow up. So, I just want to know politics, is that enough? Is that going to get us where we need to be?

JEFFREY ROSEN: Declined to have his remarks published.

JOHN KING: Here's the politics.

JEFFREY ROSEN: Declined to have his remarks published.

ATTORNEY GENERAL JENNIFER M. GRANHOLM: No, there aren't because the law is not there yet. There's no individual redress in these yet because you know it's just not. That's why our Consumer Protection Act in Michigan, we did this sort of creative spin on it. Our Consumer Protection Act is the greatest act in the world because it allows for the Attorney General to come in and negotiate with a business before filing a lawsuit. It gives you 10 days in which to respond. And under our act the failure to disclose a material fact that would lend to completion of the transaction is a violation of our act. And so it was my belief that the failure to disclose the presence of third-party cookies or tracking devices on a website was a material fact that people needed to be told about, which is why we went after the websites, the failure to have privacy policies on a select number of websites. So did any individuals get redressed? No, although the websites have all come around.

And, there was one question about what reading can be done or if there's any suggestions regarding privacy policies. In fact, as a tool we posted a couple of model privacy policies on our website that we thought might be useful for those who might be looking at this. Our website is www.ag.state.mi.us. People can go and see if there's anything there that might fit your particular

entity. But, there is nothing right now that gives an individual an ability to do that unless it reaches that highly offensive threshold under the tort law, which I think should not be there. My proposal is to take away that highly offensive threshold and allow people to be able to file for the release of personal information but not have it get to that, it has to be serious violation, but does not have to be highly offensive. But I just am somebody who's not just a thinker but a doer and I want to be able to get results. I want to be able to move this dialogue forward, which is why we've taken action in the way we have against all of these websites. We've gone after 13 now, companies, online companies, and we've selected the ones that are in sensitive areas that we believe people would be alarmed if their information were compiled onto. To push the federal dialogue forward, too.

JONAH SEIGER: There are a couple of things . . .

JEFFREY ROSEN: Declined to have his remarks published.

ATTORNEY GENERAL JENNIFER M. GRANHOLM: Sure, every move you make does.

JONAH SEIGER: Couple of thoughts in response to the Attorney General's comments. I think that going after sites that have privacy policies that don't disclose that they're setting third-party cookies is perfectly appropriate. And I think that one of the solutions to that is a standard, again, for notice and disclosure. If you're setting third-party cookies your privacy policy should say so. If it doesn't, then if enshrining that standard, for example, in federal law would give a right there. So I think there are ways to suppress this.

Another thing when you talk about the role of the courts or the judiciary there are also, and I don't want to overemphasize this especially in light of Joel Klein's comments yesterday, but there is a market force here too. There is a competitive advantage for privacy. And you start to see this, Earthlink is now advertising in its attempts to cut into AOL's (America On-Line) marketshare that they don't track you, that they're just the pure Internet. And that's actually true, although it's sort of misleading because the other sites that you're accessing through Earthlink still might. But the fact is that you're starting to see companies differentiating themselves, major access providers, differentiating themselves, on the issue of privacy. So, there are other forces here. And, again, I think to bring it down to the practical level, which I think is very important, is that if we want to continue to foster the growth of this medium and all of its benefits for commerce, for education, for democracy we need to have a way for information to flow and transactions to work smoothly and seamlessly across all 50 states let alone the entire globe, which is a whole other mess of yarn that we're not going to talk about.

ATTORNEY GENERAL JENNIFER M. GRANHOLM: Let me just respond quickly to the market based issue because I think the market has responded to a certain extent but certainly not as much as you would want it to in light of the very few people who are talking about this. The average person out there has just no idea about their activity online being tracked. We see this as we go around the state. As I tell people you know that Richard Smith testified in Congress that DoubleClick has reserved enough space for the equivalent of 300 single spaced pages about the people who have been online. Now that is a pretty darn detailed profile even if you assume that they're not putting the name and address with it, at some point if you've got my IP (Internet Protocol) address and you've got where I've been with 15 different transactions, it is one person, just one person who can do that, that triangulation of data becomes personally identifiable after a

while. But the market has not responded effectively and that's the problem. If the market were to respond effectively then we wouldn't really be having this conversation.

JONAH SEIGER: There is a model for this, though, in that there's a group called the Network Advertising Initiative that was a coalition of network advertisers including DoubleClick and they have put forward an even more aggressive position and it's controversial on both sides. The privacy advocates think it doesn't go far enough and the privacy moderates think it goes too far. But it gets to this point that the Attorney General just mentioned about the linkage of personally identifiable information with non-personally identifiable information. And Jeffrey talked about this too. This was the most egregious thing that DoubleClick did and they rightly got slammed for it. Because they were going to combine information collected for one purpose with information collected for another purpose without any knowledge or notice or consent. And so if you take the NAI (Network Advertising Initiative) model and think about a different standard-- not for the collection of information where you ask for consent, but the merger of information that's personally identifiable with information that's not personally identifiable-- create that detailed profile, that is another area where there might be some places . . . .

ATTORNEY GENERAL JENNIFER M. GRANHOLM: Now, here's my cynical hat that I wear. The NAI ended up, the attorneys general had a meeting with Microsoft to talk about their browser, their Internet explorer browser and how the defaults were set. It's so difficult to find so that you can't turn off your cookies or you can't distinguish between first-party cookies and third-party cookies. That to me is a critical distinction that the market should respond to. Microsoft said, "We will do a patch for our Internet explorer browser and enable users as a market response to have--to pull up on your default systems--the ability to turn off your third-party cookies but keep your first-party cookies so you can interact online and have a meaningful web experience without feeling like you're being tracked." They proposed the solution and NAI went nuts because this, of course, would turn off the ability of these third-party advertisers to be able to gather data especially with the 800-pound gorilla that Microsoft is. So I'm just a little cynical about the third-party advertisers and their sincerity in offering a market solution.

JONAH SEIGER: I think that's justified cynicism but look at the example of DoubleClick. I think, unfortunately, the political goodwill and political capital of that community, some people refer to those companies as the tobacco companies part of the Internet industry. But I think that we have to ask in that context: what is the difference in kind between a first-party cookie and a third-party cookie? Is it the fact that I've clicked on a page and anonymously identified myself as reading an article about the Michigan Attorney General's activities or I'm looking for a new car? With the linkage of that information to a personally identifiable activity, it's not necessarily the case that a third-party cookie is any different from a first-party cookie except that it's the way that the infrastructure has been set up. So if we demonize third-party cookies just for the sake of being a third-party cookie, I think it sort of obscures the essential issue which is the personally identifiable information and the non-personally identifiable information and the linkage of that with respect to the consumer's control of that linkage or choice for that linkage.

JOHN KING: I'm going to have to call this to a close. It's extremely interesting. We haven't really touched on all of the questions we received and we've got four more. Let me just tell you quickly what they were.

One has to do with whether or not the technology has had the effect of changing people's expectations of privacy so that itself is a moving front. Another one has to do with problems of maintaining privacy about DNA and gene information and so forth in the face of the ability to patent such information now, and is there a conflict arising with patent law there?

Another one has to do with legal literacy. Can people really understand what the privacy legislation regulations are as everyday consumers?

And finally, what happens when privacy policy can be changed unilaterally by other kinds of policies, for example, decisions of bankruptcy courts and so forth?

Please fill out the yellow form if you haven't already done so and leave it behind. This has been an extremely interesting session I'm very grateful for the opportunity to moderate it and I'd like to thank, all of us thank the Attorney General and our two discussants. Thank you very much.

(APPLAUSE)