Information Access in an Electronic World

An E-Government Policy Panel

Summary Transcript

Center for Technology in Government
University at Albany / SUNY

Information Access in an Electronic World
An E-Government Policy Panel

Summary Transcript

On January 17, 2002, an information policy panel discussion was sponsored by the Center for Technology in Government in partnership with the New York State Forum for Information Resource Management. The following is an overview of the issues and an abridged transcript of the panel discussion.

The Issues

Information policy issues did not emerge with the Internet. Freedom of expression and the commitment to open government have been with us since the beginning of the Republic. Policy attention to information issues has been dramatically heightened, however, by the events of this past fall. Since then, our news has focused on public safety, homeland defense, counter-terrorism and related topics that generally engage only a few government agencies. With the new focus on domestic security, the mainstream activities of government -- educating kids, assuring health care, building roads, collecting taxes – face new information policy responsibilities as well. In this security-conscious environment, how should government leaders and managers think about policies to guide information collection, management, access, and use? How can we balance inevitable conflicts among privacy, public access, and information ownership?

Information policies fall into two complementary categories: stewardship and use.

The "stewardship" principle is a conservative one that focuses on quality, integrity, security, reliability, and documenting and maintaining the public record. It treats information as a "public good" -- something that needs to be nurtured, maintained and protected on behalf of the public.

The "use" principle is an expansive one. It treats information as an asset that we use to achieve any number of public goals. It focuses on the current and the future value of information, the ability to share, integrate, and reuse information. The use principle leads us toward innovation, the development of new or better services, lower costs, and new relationships with citizens.

In the context of these two complementary ways of thinking about government information, the panel explored questions of access to information on the Web, proactive dissemination of government information, database integration, information sharing across organizational boundaries, the new emphasis on identity, and system and data security.

The Panelists

Debra Cohn is Deputy Attorney General for Policy for New York State. She has been a Special Counsel to the Deputy Attorney General at the U.S. Department of Justice, an Assistant United States Attorney for the Civil Division, and a law clerk to Justice Thurgood Marshall. The Attorney General's involvement in information policy is multifold: the office represents state agencies in litigation over information policy issues, such as the Freedom of Information Law (FOIL) and the Open Records Law; the Criminal Division prosecutes fraudulent activities against the state; and the Public Policy Division examines actions by companies that violate privacy policies.

Alex Roberts is Assistant Director for IT Services at the Division of Criminal Justice Services. He is responsible for systems development, integrity, and security and IT services. The Division of Criminal Justice Services manages information to enable the smooth functioning of criminal justice in New York State. The Division maintains a statewide, automated fingerprint identification system that is tightly integrated with the criminal history database. The Division also processes and coordinates a large volume of background checks on people applying for certain jobs and licenses in the state.

Julie Leeper is an Assistant Deputy Director in the New York State Office for Technology (OFT) for Strategic Policy, Acquisition, and e-Commerce. She is responsible for leading New York's "Government Without Walls" e-government/e-commerce initiative. The Office for Technology is responsible for statewide information technology issues and works with state agencies to develop information services and policies that support the effectiveness, integrity, and security of electronic services.

John Sennett is a Special Agent for the FBI in Albany and has been with the Bureau for 22 years, including assignments in counter-intelligence and counter-terrorism in Cleveland, Washington and New Haven. In addition to his work as an investigator in the field, he provides training in state and local law enforcement and emergency management organizations. One role of the FBI is to detect, deter, and disrupt terrorist elements before they can strike in the U.S. To do this effectively, the FBI must address basic information policy issues, including government data integration, personal identification and privacy.

Ari Schwartz is Associate Director of the Center for Democracy and Technology (CDT) in Washington. He is an expert on privacy and has testified before the Congress on these issues, particularly with respect to the use of the Internet by government agencies. CDT is a non-profit advocacy organization that focuses on bringing communications technology to its full democratic potential. CDT works with industry, government, and public interest groups to defend free expression and open government, and to develop effective privacy and security policies.

The Discussion

Sharon Dawes (CTG, Moderator): Making government information widely accessible over the Internet has become controversial since September 11 and many agencies are re-evaluating their Web site content -- what are the benefits, risks and trade-offs of broad content and access? What criteria should agencies apply when adding or deleting content from their Web sites?

John Sennett: This is a common sense issue and a sliding scale issue. The ideal, of course, is complete transparency of government to the people who pay for it and are served by it. It would be ideal if everything you ever wanted to know about New York State Environmental Conservation or the United States Environmental Protection Agency was on their Web site, and you didn't have to go to the library or get on the phone or write them a letter to get any of their manuals. It would be ideal if everything you wanted about an agency was on the Web site, including a full description of all the staff. That would be ideal -- aside from the fact that it raises obvious security problems. A rule of thumb is that a Web site should contain all of the information that a reasonably diligent citizen could get by going to a public library, but certain obvious things should be deleted.

Julie Leeper: The initiative that I'm most familiar with is our e-commerce/e-government initiative, and our goal is to make information available to anyone, anywhere, anytime -- 24 /7. That means getting information to the public, and letting citizens, other levels of government and businesses access services whenever they want. It also includes stewardship of the infrastructure, providing a secure network and ensuring that transactions are safe. We need to know we're providing the right security when we provide a service or transaction. If we have the right security, then we can also provide privacy to citizens and businesses. There is a need to do risk assessment. When you look at providing information or a transaction, you have to ask "what is the risk?"

After 9/11, our office sent out a memo to all the state agencies asking them to do a review of their Web sites. The directions we gave them were to look at things like detailed building floor plans that showed every exit, every floor, every emergency exit, and every elevator. The general public really doesn't need that kind of information. We asked 72 agencies to complete reviews and 10 agencies took some type of information off. This doesn't mean the public doesn't have access to information. They can request that information. It just may require some type of authentication or identification so that we can trace that back to who received that information.

Debra Cohn: We have a strong legal framework to help us with these questions and past experience representing state agencies on information policy issues. For example, if an academic or a reporter

studying flood planning sues the State Emergency Management Office for removing Web site information about emergency stockpiles and water pumps, the Attorney General's office would serve as the State's counsel. We would wrestle with the provisions of the U.S. and New York State Constitutions and examine the statute, and then we would work with the agency managers and counsel to address the issues.

There are other concerns that might affect the contents of a Web site or information made available to the public. For example, our office did a study of election law, and suggested that there be a computerized voter registration list for the state. It would enhance voter participation and help detect voter fraud. But there's a lot of private information there, and it would be available to lots to people, for illegal as well as political and commercial purposes. So it's not just security that must be balanced against making all public information available to everyone. Privacy matters, too.

Ari Schwartz: It does go a little bit beyond common sense. Seven years ago we advocated for guidance for what information went up online, particularly around the time when the army generals' Social Security numbers were being posted up online by well-meaning people in some different offices. But at that time they said, "Well, the policy's been let a thousand flowers bloom." And now we are basically giving out pesticide to everyone and letting them sprinkle it wherever they want.

There are many things that could be considered security threats: bus schedules, public meeting points. Just because it's a security threat doesn't automatically mean that it's taken down. What's the balancing point? Common sense has changed quite a bit since September 11. How should rules be set in a way that is balanced? Guidance is necessary.

Moderator: Proactive dissemination of government information is a means to educate and inform the public, especially in times of crisis and change. In what ways can state and local agencies use their information to keep people well informed? What partnerships (with the media, for example) make sense in this educational effort?

Julie Leeper: Using 9/11 as the example, I came up with six categories of information that was disseminated over the Internet. The Internet was used to broadcast reassurance and leadership messages. The governor issued many press releases after the event, as did the mayor. There was also an address to the Legislature available on the Internet. The Internet provided direction in New York City. MTA (Metropolitan Transit Authority) had where the subways were going or not going, the adjusted schedules, the relocation of offices for employees. The Internet was also used to provide directions for people about how to get information about their family members. Web sites were also used to broadcast changes in

normal procedure, such as an extension of tax deadlines and exceptions on getting death certificates. It provided ways to help. People wanted to volunteer. They wanted to do something. How can you volunteer? How could you make donations? The Web was used for that extensively with 9/11. It was also used as an outlet for expression of concerns and thoughts. People used the state portal for this. They didn't know where to go. We don't have a direct e-mail on the portal. We have a feedback form and people just used whatever open block they could and typed messages of condolences from all around the world. And lastly, it's a way to let the public know when things are back to normal.

Moderator: Considering the continuing problem of the digital divide, what means, other than the Internet, should we be promoting to give people better access to information? In a related question, what do you think should be done to make people more aware of government information and services on the Internet?

Ari Schwartz: At CDT, we look at the digital divide the other way around. We focus more on how to get people who don't have access to understand how the Internet works and how to get public access to it. Recently we have seen the gap closing to some degree, but the literacy gap has not closed as much as we would like. But it really has to be an important issue, especially in light of how more services are moving online.

In terms of getting greater awareness of what's out there, that becomes much more difficult in the budget situation governments are in right now. We need innovative ways to get the information out there because it is so much cheaper to access information services online for both the government and the citizen. There should be a push to get people to use these systems to make them more worthwhile.

Moderator: Interagency and intergovernmental information sharing was crucial to the response and recovery efforts following 9/11, yet it remains a very difficult challenge throughout government. What are the key barriers? Will our recent experiences help break them down? Would new information policies make a difference?

Alex Roberts: From our perspective in Criminal Justice I think the barriers are the same in all areas of society. They all go back to the most basic thing – we have to speak the same language. This is true whether it's two human beings that have to communicate or whether it's computerized systems. We need protocols for communication and standards for passing information to be able to interface our systems today. Data standards and open protocols are not particularly the first things people in technology want to work on, but they are critical.

The data that is passing between connected information systems has to follow the same standards all the way back to wherever it's collected manually. All the information, let's say on an arrest fingerprint card, has to use the same data elements all across the state, all the way through the system. This is critical now that we are starting to tie systems in different parts of society together. On 9/11 it wasn't only criminal justice that had to respond. The health system and the social services systems also had to relay information to get the job done.

Up to now there have been half-hearted and partial attempts to create standards that cross all of these boundaries, but they have not been fully successful. I believe government will have to work harder at this – all areas of government, federal, state, and local. It can only be done collaboratively. It's never worked by dictating from the top down because people just don't accept that.

John Sennett: At the present time the major threat to the security of the United States and its people is international terrorism. In the world that we would prefer to work and live in as American citizens, when a trooper on the Northway in the middle of the night pulls over a car and says "License and registration, please," he should be able to look at the driver's license and be able to say, "I see that you're a foreign national, and according to this license your visa has expired. You're going to have to come with me." Not because he was going five miles over the speed limit and not because his taillight was out, but because he was in the United States illegally. That is not a trivial offense anymore.

The only way that trooper can know that the driver is in the country illegally is if the U.S. Immigration and Naturalization Service (INS) shares its data with the New York State Department of Motor Vehicles and that's never been done before and it's not going to get done tomorrow unless we have the political will.

Alex Roberts: We have also approached these problems of information sharing through the Legislature. For example, they took up the question as to whether it is appropriate to share information about juvenile offenders. So I'm sure the Legislature will be considering the issue of whether or not it would be appropriate to share our criminal history information with the INS or vice versa.

Debra Cohn: There are also turf battles with sharing of information from government agencies. Calling it turf may sound pejorative, but there's a great deal of pride in creating a database and in making sure it meets certain standards. The collaborative process is not just coming up with shared standards, but also trust in the different people who share the databases and apply the standards.

Moderator: Some people are calling for greater integration of government databases for easy access and cross-checking by public agencies, especially for public health and law enforcement. What are the benefits and risks of doing this? What safeguards need to be applied?

Debra Cohn: We all come to this with a presumption that there is a great benefit in integrating government databases that serve similar functions, such as law enforcement databases. For example, I did some health care fraud enforcement and literally the investigators could not look electronically at whether providers were double billing in terms of Medicaid and Medicare because the systems weren't compatible. We had to do that manually and that was a terrible impediment to enforcement.

There are a lot of challenges here. Databases are usually created from the ground up and have different demands for the data entered into the system and the quality of the data. Even within law enforcement, data is obtained using different tools and those tools may only provide us with data for certain purposes. There are lots of different limitations by which government obtains data and they all affect and limit how that data can be integrated.

Another issue is privacy. I'm originally from Australia. They have fewer problems with health care fraud enforcement because they have a single-payer system. They have every single patient and every provider in one database. Well, that story usually makes people sit up -- "You mean someone could know exactly the prescription drugs I'm taking and what doctor I've seen for what purpose?" It may have certain benefits but it raises some serious challenges as to whether we want government to have all that kind of information.

Moderator: Personal identification and privacy. In what ways should government safeguard personal identity and personal records? Do we need a national identity card? Is personal privacy a casualty of 9/11?

Ari Schwartz: I think the initial questions should be: "What is the problem that we're trying to solve with a national ID card?" and "Will a national ID card be effective in solving that problem?"

The public has been very supportive of the idea of a national ID card because in theory it sounds like it would solve a lot of the problems, but in practice it would not solve the problem we had on September 11. The attackers on September 11 would be in a national database. They would have legally gotten the card and would be able to use it. Instead of focusing on trying to integrate the identification data into a single place, we should be focusing instead on how to get better standards for ID card registration across the country.

Julie Leeper: Just this week the American Association of Motor Vehicle Administrators (aamva.org) came out with their recommendations. AAMVA is an association of motor vehicles agencies across all 50 states and Canada. They're not looking at requiring biometrics because that would cost many millions of dollars, but at merging different technologies. The choice would be up to the consumer. They would bear some of the cost. It depends on how secure they want their card to be in identifying themselves. It could be biometrics; it could be simple bar codes; it could be PINs. Do they want additional private information to be stored in that national or state database? It would be their choice.

Alex Roberts: I have a comment that's not technical, but sociological. The vast majority of us have agreed to live our lives by the social compact. We're part of a community and all of a sudden we're face-to-face with people who aren't following the social compact. Now we're trying to come up with technical or social conventions to deal with that issue. We're moving from a village perspective to a world perspective. It used to be very simple to say who's part of my community, who's part of my tribe, who's part of my little cave group. Now our community is the world, and if we keep coming up with technical solutions that don't account for the whole global community, then we won't be able to adequately address the problem.

Moderator: Do we have to trade privacy for security? According to polls, "We're willing to give up more of our privacy for more security." Are we really? What are some of the issues here?

Ari Schwartz: There is a balance. Recently a lot of the agencies have gotten the idea to do these risk assessments -- privacy and security impact assessments -- in the same way that we do with environmental impact assessments. That has been a major step forward. But in other instances, the funding of these assessments has not been addressed at all. For example, the INS has completely antiquated computer systems. They have not done any kind of privacy-security analysis because they don't have the funding to do that.

Ninety percent of the USA PATRIOT Act was not controversial. For example, it increases the budget of the woefully under-funded FBI computer crime lab. However, there were also provisions in there that we have major concerns with, especially those overriding privacy laws, the state privacy acts, the library records privacy laws, etc. Also, it removed much of the oversight by the judiciary so it gives law enforcement more unchecked powers. Now it becomes harder to monitor because it's no longer going through that independent judiciary. So we are concerned that that balance has swayed off, particularly in the wiretapping area. It's something we're going to have to monitor carefully, despite the fact that we've lost the formal power to do that monitoring.

John Sennett: We're faced with a situation now where the American people want us to detect, deter and disrupt terrorist elements before they have an opportunity to kill us. And that's entirely rational. But it does create tremendously difficult and complicated problems. How do we, as a government that keeps data on people, mine that data if they haven't done anything wrong? We don't investigate people in our country who haven't done anything wrong or who haven't conspired to do something wrong. By the time somebody is conspiring, the thing that they're going to do might be only a week away and it might take 3,100 lives. But I agree that the thing that holds our system together is judicial scrutiny…skeptical judicial scrutiny.

The FBI must go before a judge and say, "Your honor, we need to identify e-mail traffic between her and him." And the judge says, "Well, why do you need to do that? Why do you think they're engaged in something that is criminal?" And we have to explain why we think it's important that we have the e-mail traffic between her and him. And then we have to explain to the judge how we are going to sort out only her e-mail traffic that goes to him and only his e-mail traffic that goes to her. Every 30 days or 60 days, when the warrant has to be renewed, we go back before the judge. Judicial scrutiny is what keeps police powers from being abused more than anything else and we shouldn't let it go.

Moderator: Security of government networks and information systems -- what are the threats? How safe are they today from intrusion and damage? What mechanisms need to be put in place to assure system and data security? Can strong security and ease of use live side by side?

Alex Roberts: Nobody doubts that if the entire telephone network in New York State went down it would be a massive attack on our national or state infrastructure. If our information networks, whether they're the Internet or our information systems, went down, it would really impact our day-to-day lives. Today we've made decisions such as merging our e-mail networks in our agencies. They may be the same networks that our criminal justice or health or social services information is on. If somebody happens to get a virus or an e-mail that takes the whole network down, it doesn't just take down e-mail, it takes down the information system that is the bottom line of our services. That's why we all need to care -- and why policy makers need to care -- about security.

John Sennett: They're not very safe. Networks are safe if no one is attacking them. But apparently there is an endless supply of hackers of varying degrees of evil who seem to take a special delight in, and are willing to spend hours, trying to penetrate systems. Young people come home from school, put down the

backpack, go upstairs to the den, and get on the computer and just hack and hack. And in the FBI we're worrying about Col. Khadafi hiring a team of hackers and we'll probably see that some day.

Julie Leeper: Our information security officer monitors hackers' discussion groups. She's watching what the hackers are talking about. We need to understand their mindset. The key is absolute diligence, constant care, and watching. We can never stop looking at the logs. It's a tedious job and that's what the security officers need to do. We don't put a security officer system in place and move on to the next project, it's constant.

Moderator: Carolyn Purcell, the CIO of Texas, says the real security problem is not technical, it's getting people to appreciate the importance of security and to behave in ways that are different than they're used to. Can security and convenient ease of use in systems live side by side?

Alex Roberts: Whether it's for privacy concerns or for security concerns, we have to strike a balance. We have been merging systems to make information flow easier and to save money. But from a security perspective, if we have an information system that has a much higher risk and degree of security, it should be compartmentalized. That may even mean that we need to have separate logical or physical networks that carry that information. We have to take a strong look at it and sometimes say, "Well, less ease of use will satisfy not only the privacy concerns of people but also some of the security concerns." It may be that we do some more compartmentalization than we would have otherwise.

Moderator: Should we be doing security clearances or background checks for people who are responsible for systems?

Julie Leeper: In the Office for Technology, all of our professionals are ID'ed and fingerprinted. It's not an overall statewide policy, but I've worked in four agencies and in two of those four agencies fingerprinting was a policy if you were in a policy-making position or a steward of data of any secure nature. So I think that's already happening in a lot of agencies.

Alex Roberts: It's often quoted that greater than 80 percent of all security intrusions and threats take place from internal employees. But I think we will also find that in a vast majority of those cases there is no prior criminal record or prior criminal history. That doesn't necessarily mean that that's an indication of the security worthiness of an employee. That's why we train employees in the appropriate use and signs of abuse of information. Now on the issue of staffing, frequently we think of government agencies in terms of their service missions. But most, if not all, of our governmental institutions today are critically involved with information, not just services. The services depend on information and information systems. And we

can't stint the human beings that run those information systems or keep them from moving forward without having an impact on the bottom line of the services.

Moderator: What's the one most important thing that you want to say, the most important message that you want to leave the group with today?

Ari Schwartz: The most important piece is trying to figure out the optimistic way to look at this situation we find ourselves in. We discussed the way that the Internet functioned during the crisis and how can we build on that. Another example is in the context of the anthrax threat. It was difficult to deliver mail to federal buildings. In fact, Congress still isn't accepting its mail today. But also we know that traditionally constituent services have been very poorly managed. Traditional mail, electronic mail, and telephone calls are all treated differently. They go through different systems and people. Is there a way that we can use this crisis to reevaluate these kinds of constituent management systems and create something that treats all different media in a similar light so that it goes to the right person at the right time? We have a chance to completely reevaluate the system and take away some threats. Obviously there are costs to that. But if we're spending all this money irradiating mail, perhaps we can streamline the entire system and save money down the road.

John Sennett: Security is a pain in the neck. It's time-consuming. It's tiresome. It doesn't contribute to productivity. It's just downright annoying. I've got about six passwords and I have to change them every week. I can never remember them. But we have to find ways to go about our daily lives and make a living and get business done and enjoy living in America and still be safe. We have to put on our thinking caps in the next decade or two to find ways to utilize technology to make our lives safer without fraying the Bill of Rights. We have to be safe enough to meet current and reasonably anticipated threats and the only way we're going to do that is to utilize security intelligently and comprehensively.

Julie Leeper: We need to continue to move forward and make government information useful and accessible. But we have to keep our eye on stewardship. We should not take the easy way out and just say security's too hard; we don't have the budget; we don't have the money. If that's the case, then we cannot move forward in a balanced way. When we can't deliver physical mail to a building, send e-mail. We can do that in secure methods and there are technologies like encryption that can enable us to be stewards. We need to encourage leaders not to take the easy way out, to listen to security officers, to strike compromises that balance risks.

Alex Roberts: When the farmer kicks over the ant hill, the ants all come scurrying out and scurry around for a certain period of time; then they go back to their business. When we have a huge crisis like 9/11, society comes out and posts police officers in front of every governmental building for a while and then slowly people go back to business. And why is that? Because a lot of times how we react as a society and as individuals is not sustainable. We have to come up with, and put in place, sustainable measures that don't fall away as the months from crisis go on. We have to think about how to keep this going. How will we sustain this effort so that it really makes a difference three years from now when the next crisis comes along?

Debra Cohn: I wanted to quote two Boston lawyers who were writing about "recent inventions and business methods that gave them pause." They wrote that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops." This quote was written in the 1880s, and the reason I read it is that while concerns about privacy and security are very vivid to us right now, the concerns are not new. My message is look to what has given us great guidance -- the Constitution and other statutes. If we wanted the greatest privacy in the world, we'd sit in our homes, lock all the doors, never go out, and we wouldn't talk to anybody. But that's not how we want to live. We need a balance that reflects the traditions of democracy and security that are already embedded in our Constitution.