



Homeland Security

The Privacy Office
Department of Homeland Security
Privacy and Technology Workshop:
Exploring Government Use of Commercial Data for Homeland Security
September 8-9, 2005

OFFICIAL WORKSHOP TRANSCRIPT

Friday, September 9, 2005
Auditorium
GSA Regional Headquarters Building
7th and D Streets, SW,
Washington, D.C., 20024

CLOSING REMARKS

Chief Privacy Officer
Nuala O'Connor Kelly

MS. KELLY: Well, first let me thank the final panel. I think they did a great job. [Applause.]

MS. KELLY: It's always a great part of your day when you get to learn from people who have thought more or better or longer about these issues, and I think that was the selfish reason behind why we had this conference. We were able to bring wonderful people together and hear from them, as well. Someone inside the Department asked me, rather pointedly, recently, after seeing our invitation, "Well, why are you doing this workshop?" We see it as part of our mission. Our mission at the Privacy Office is to be both within and without this Department. And what we mean when we say that is really that we are part of the operations of the Department of Homeland Security. Our operation is to enforce privacy protection and privacy practices. But it's also our mission to bring the outside in, to bring the critics in and make their voices heard within the Department, in the agency, in a way that Department leadership can understand and hear.

I think parts of these dialogues are not only our mission to serve you, but our mission to serve the Department, too, to make these concerns heard and realize and make them operational in the future. I think this is only the first of a long dialogue towards that goal. It occurs to me that we are all serving, in our way. I worked for a woman, many years ago when I was in college, who said that, "There are many ways to serve this country. You don't necessarily have to work for the government. It can be on the outside,

DHS Privacy Office: Privacy & Technology Workshop

September 8, 2005 Official Transcript

as well." And I think everyone who's participated in this conversation, both on the stage and in the audience today, is serving their government in a way by having the dialogue, by criticizing, by applauding, when appropriate.

So, let me offer just a few of my thoughts on this dialogue, in summing up and having learned a great deal. I think that the questioner who asked, a few minutes ago, whether we shouldn't really go back to the threshold question of, "Is this even a good idea?" -- that's exactly right. I think having a toddler around the house makes you remember to ask the simple questions, the basic questions, like, "Why?" Why is this a good idea? Is this necessary? Should we be using commercial data or outside partners? And my answer -- I think the rest of my remarks will either please or disgruntle almost everyone in the room, so I beg your indulgence. I would argue that there are some valid uses of commercial data. There is great ingenuity in the private sector. Most of you know I've spent more of my career in the private sector than in the government, and I'm aware of the speed and the agility and the excellence with which the private sector can move forward, not only in its development of technology, but its ability to process data and to, hopefully, get the right answers. And their financial incentives also often are in that direction of excellence and quick movement. We've certainly seen that in our response to Katrina. The need to rely on private-sector partners to help, to move quickly, to get information to first- responders and to shelters and to people in places where they need them at a time when sometimes communications are failing us.

I was really struck by a number of companies -- I mean, even companies like Wal-Mart, who I think offered to employ their employees wherever they showed up in the country, which I thought, that's really spectacular. People need jobs at this time. They need housing, and they need food, and they need jobs. A few others came across my desk, and I thought you should know about some companies that have volunteered their services free of charge or as part of existing contracts. My friend Phil Bonds, who's now at Monster.com, was one of the first people on the scene to say, "We've got technology that can link people together. Usually we use it for jobs, but let's use it to link people with their families." Let people get online at the shelters and wherever they are in the country, the libraries, and say, "I'm here, where are you?" And, you know, I thought, that's really a great public service.

And ChoicePoint, which has been mentioned a number of times in the last few hours, stepped forward with mapping technology to say, "Where are you? Where are the first-responders? Where are the evacuees? Where are the nearest shelters? And where are the nearest doctors?" I mean, that's really front-line stuff that I think has been essential. And they've also offered some of their technology to state and local first-responders to provide identity verification management. So, you know, there are -- there are good, valid uses of this technology, as well. IBM too has offered, as both -- not only an existing great

DHS Privacy Office: Privacy & Technology Workshop

September 8, 2005 Official Transcript

contractor of the Department, but it offered a number of new technologies to put people together at a time when they have lost everything.

So, the challenge, I think, is to ask the question which has been raised over and over again: Why? Is this a good use? Is this a good purpose? And does this technology and this data work to that end? Is it a valid use of that technology and that data for that purpose? And I think that's, obviously, a threshold Fair Information Principle question and a threshold public-service question for this Department. Given -- if we have established then, a legitimate public policy use for data, whether its source be within or outside the government, then what are the policies and practices and procedures that we're going to have in place to constrain that data?

I would argue --and some of you will see my, perhaps, libertarian bent here -- that I would say the best protection is for the government not to have the data for any great amount or any great length of time. But that's not to say that we want to go around the Privacy Act by using commercial databases or other sources in a way that skirt that law. On the contrary, I'm saying let's use basic holding and processing constraints to limit government's access to information, whatever the source. And, assuming that all of that is done, then the other kinds of fair information principles of access, redress, accountability, I think, will only increase public confidence in our Department and in the use of both commercial and government data.

And, of course, I was gratified to see that we ended on the note of oversight and accountability and auditing, which is very much how we position ourselves in the Department. People have tried to define our Office as the Inspector General or not the Inspector General, the General Counsel or not the General Counsel, but we are, fundamentally, a privacy operations and oversight office. And I think -- I humbly would submit that we have created a paradigm for other agencies to possibly follow, as well. I'm incredibly proud of the people we've got on our team working every day side by side with our fellow Department of Homeland Security employees, and I think that we have enforced a discipline. That's not to say we're perfect, that we don't have a long way to go. There's always more to do. But I'm proud of the last two years, and I think we've got our work cut out for us for next. Thank you very much. [Applause.]

MS. KELLY: And thank you -- one last note to Toby Levin, who is probably exhausted at this point, and to our whole Privacy Office team, thank you very much. [Applause.]