TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTIONS FOR ID AUTHENTICATION

PANELS 1 & 2

APRIL 23, 2007

>>JOEL WINSTON

Welcome to the FTC and our workshop on *Proof Positive: New Directions for ID Authentication*. I'm Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the FTC. It is my pleasure and honor to introduce Chairman Deborah Majoras of the FTC. Chairman Majoras was sworn in in August 2004 as chairman of the FTC, and among many other achievements and honors she is serving currently as co-chairman of the President's Identity Theft Task Force that was established back last year. So without further ado, Chairman Majoras. (Applause.)

>>CHAIRMAN DEBORAH MAJORAS

Well, thank you very much Joel, and good morning everyone and welcome to Washington and to the FTC. Your presence here, whether here in person or via the webcast, is very, very important. While strengthening the authentication process offers great promise for reducing the misuse of consumer data it will require a lot of creative minds and a great deal of coordination.

A short time ago it was reported to the FTC that a soldier returned home from deployment in Afghanistan and tried to access his credit card online. When he was denied access he contacted the issuing company and discovered that while he was away someone had changed the account number and the billing address, and when he asked how this could have happened he was told that the company received the change request through a phone call so they changed it. Fortunately, he was then able to get the account closed, reverse the fraudulent charges, but the delinquent account and the suspect's address had already been reported on his credit report so he had that entire mess now to contend with. Surely we can say that this soldier deserved a better welcome back home.

While we have done much over the last decade to protect consumers from the harm associated with identity theft, much work remains to be done. This workshop is the first of the many steps we intend to take to make sure that stolen Social Security numbers or other personal data will no longer be used as the keys to a consumer's identity. Last September, the President's Task Force on identity theft delivered several interim recommendations, including convening this workshop to focus on promoting better ways to authenticate the identities of individuals. That Task Force recognizes that authentication, insuring that a consumer is who he or she purports to be, is a critical part of the life cycle of identity theft.

Now any discussion of authentication is inevitably going to revolve around technology, and a quick scan of our agenda over the next two days would support that conclusion. But we must always remember that the workshop is about consumers and how we in government, you in industry, can use technology to protect them from identity theft.

No one would argue, of course, that identity theft only harms the individual consumers. In many cases businesses bear the brunt of the financial loss. But what may have a greater lasting impact than the direct cost of ID theft is the damage that it does to our economy by threatening consumers' confidence in the marketplace generally and in e-commerce specifically. A recent Wall Street Journal/Harris interactive survey found that as a result of fears about protecting their identities, thirty percent of consumers polled were limiting their online purchases and 24% were cutting back on their online banking. Our economy, indeed our society, is built on trust. Trust that consumers will fulfill their obligations; trust that industry will respond to consumer demands; trust that government will protect the well-being of consumers financial or otherwise in the event of market failures. Identity theft undermines that trust.

We recently received an identity theft complaint from a young consumer who recounted his experience of going with his mother to open his first checking account before he headed off to college. At the bank, he learned that a woman using his Social Security number had already opened a checking account which had been subsequently closed for default. When he contacted us, this young man was still working to clear his record. It's hard to regain trust in a system that allows that kind of a breach. So if you multiplied this consumer's story by the thousands of consumers that we're hearing from every week for an instant calculation on the scope of the problem we are here to address.

Some decades ago if you wanted to buy a house or start a business, you usually went down the street to your neighborhood bank where they knew you and would decide whether you personally qualified for the loan. Of course, the modern American credit system relies on the gathering and dissemination of information related to the experiences of multiple businesses with the credit worthiness of the consumer both positive and negative. This information enables businesses to assess more accurately the risk that a particular consumer will not meet his or her obligations without actually having to know that consumer personally. Consumers have reaped enormous benefits from this system in terms of increased access to and lower prices for credit.

We've learned, however, that the benefits do come at a price. We know people now buy bits and bytes of information. How can we be sure that the person presenting the information is in fact that person the information belongs to? The gap between our actual selves and the information that represents us is precisely the gap that has nurtured identity theft. I'm not talking about avatars, I'm talking about us and our information. It's a gap that needs to be closed if we are to make significant headway in our goal to reduce the incidence of identity theft.

Now at the same time, of course, we don't want to create even bigger problems. With the benefit of hindsight we have much to learn about our past use of Social Security numbers, often the most valuable piece of consumer information for a thief who plans on assuming another's identity. Originally created, of course, to track workers' earnings for Social Security benefit

purposes, this number has evolved into a widely used identifier adopted by the public and the private sectors to identify consumers and match information to them and it has been very useful in doing that.

But identity theft (inaudible) when we assume that the Social Security number was actually secret, and could be accepted as proof of identity. Of course, we realize now that it is not possible to use something so widely and so openly and expect it to remain a secret. Thus both public and private sectors have begun to take precautions regarding the use of Social Security numbers and many government agencies, universities, and businesses are moving away from using it as the only authenticator.

What if we had considered the impact of the Social Security number before its use became so widespread. Would we have built in greater protections or better authentication measures? Fortunately we learn from experience--I sure hope we do. And we know that we must do better at anticipating the ramifications of any new identification and authentication systems that we're beginning to build today. During the next two days we will be looking at how to develop identification and authentication systems that meet the needs of consumers, government, industry and other organizations. We must identify the obstacles inherent in building efficient and accurate systems as well as potential solutions.

Likewise, we will discuss how government and industry can work together to maximize the value of the technologies. How do we develop a coherent strategy to improve our identification and authentication systems? Is there a role for government in fostering market incentives to achieve the goals? And how can we insure that consumers will embrace the solutions once they are developed given that, without consumer acceptance and trust, no matter how superior the technology is it won't succeed.

This morning we will begin by hearing from two fellows from the London School of Economics who have advised a number of governments on the process of developing better systems. They will illustrate the need for formulating clear objectives and principles, establishing trust among stakeholders, and identifying the roles of the public sector, the private sector, and consumers. For the remainder of the morning the panels will examine the architecture and the objectives necessary to identification and authentication systems including an examination of how current identification initiatives meet these objectives. In the afternoon we will look at some of the strengths and limitations of current technologies following a discussion of the challenges of implementing the technologies as a business model.

Then tomorrow we will learn about some of the upcoming challenges we face in the mobile commerce space. We will conclude this workshop by looking at the ideas and issues raised in previous panels and attempting to propose some practical solutions or best practices for further consideration. And finally, based on the strong interest we've had in the event, we've added a number of break out sessions to the agenda to allow participants to delve more deeply into some of the issues that will be raised throughout the workshop. We're really looking forward to having a quite lively and productive debate.

The bottom line is that it is essential to coordinate our attack on identity theft. Making it

more difficult for criminals to get the information they need to steal identities is one critical piece of an overall strategy to attack ID theft. Making it more difficult for criminals to misuse the information if they do obtain it is another. We can do this by improving our identification and authentication systems so that identity thieves will not be mistaken for the persons they're trying to impersonate.

When I think about that soldier who returned home from Afghanistan, the point that stands out in my mind is how bewildered he was at the ease with which someone could be taken for him, or better yet mistaken for him. We owe him and all of our consumers an obligation to make identity theft as difficult a crime to commit as possible.

Later today I will return to this podium with task force -- with the Identity Theft Task Force chairman Attorney Gonzales, and we will formally announce the release of the Identity Theft Task Force plan. This plan is the result of careful and detailed work by seventeen federal departments and agencies and there is no better setting for its formal launch, I think, than here among those who are committed to working on this problem.

The plan identifies improved authentication as a vital key in addressing ID theft and I'm certain that the work you're discussing today will help us all implement systems and processes to allow us to take a big bite, I hope, out of identity theft.

Before we begin I'd like to thank each of our moderators and panelists for being here for your thoughtful contributions and efforts to make this a successful and productive event. Many of you, including our lead off speakers have traveled great distances to be here and I'm quite grateful. I also want to commend the FTC team that put this together. Naomi Lefkovitz , Joanna Crane, Kristin Cohen, and Stacey Brandenburg, and Alicia Mazzara. And with that it is my great pleasure to turn things over to Naomi and again thank you for being here. I wish you a good conference. (Applause.)

>>NAOMI LEFKOVITZ

Thank you Chairman. I'd just like to echo Chairman Majoras appreciation of everyone's attendance today and our moderators' and panelists' efforts to make this a dynamic and informative event.

I just have a few announcements for the panelists and the audience members. The workshop is being webcast and will be available for viewing at the workshop website in the future. The breakout sessions tomorrow afternoon, though, will not be webcast. Because of the webcast, we ask the panelists to stay close to the microphones and speak clearly. We also have a lot of ground to cover today, so please adhere to the time limits discussed with your moderators for your opening statements and please be mindful of time when answering questions to ensure that your other panelists can express views, too.

You will notice in your packets that there are some pages for notes. In particular, one page is labeled for panel 7 and is marked out with two columns. In panel 7, we would like to engage in a discussion about the issues raised throughout the workshop and consider practical

ideas for moving forward to address these issues. To that end, we hope that if an idea occurs to you that you will note it on this page and then raise it in panel 7. So we encourage you to do that.

We also hope to draft a report based on this workshop and we'd be interested in any additional observations or comments you may have. Comments can be posted via the workshop website, which is accessible at www.ftc.gov, and you may also mail comments to the address listed on the workshop website. That deadline will be May 25th of this year. Also, please visit the materials table in the hall as you will find a variety of relevant information, including this paper, *Identity Policy: Risks and Rewards*, which our opening speakers developed for this workshop.

A couple of housekeeping notes. About security: if you are leaving the building for lunch or any other time, you will have to be re-screened through security to re-enter. So please leave enough time for that. For security reasons, please wear your name tags at all times. If you notice anything suspicious, report it to the guards in the lobby. Please turn off or set to vibrate your cell phones or other devices. And please do not use the cell phone in this room as it interferes with the video equipment. But you may use the phone in the gallery area. The bathrooms are located across the lobby. It's important, so listen carefully. You're going back towards the security screening, then you make a left and they're straight ahead. Do not turn left immediately upon exiting this conference center; otherwise, you'll set off the employee card readers. That's our authentication.

Fire exits are through the main doors at the front of the building on New Jersey Avenue and through the pantry area right behind you to the G Street corridor and out G Street. In the event of an emergency or drill, we would proceed to the building diagonally across Massachusetts Avenue. Welcome to Washington, D.C.

As the Chairman mentioned, there will be a press conference this afternoon. It will be during the lunch break, so we will be using this room for that large conference. We appreciate your cooperation with the security around that event. We will be starting a little bit later because of that, so we will see you back here at 2:15. And finally, I would like to thank Microsoft for providing the coffee and bagels this morning.

And now, without further delay, let me introduce Simon Davies and Gus Hosein from the London School of Economics, who will highlight some of the issues that we will be discussing throughout the workshop.

Simon Davies is the director of Privacy International and a visiting fellow at LSE. He specializes in privacy and the impact of technology on society and individuals. His research areas include the development of new surveillance systems and techniques, the evolution of international governmental cooperation, the regulation of privacy oversight and protections, the development of surveillance over electronic media and the use of technology as a method of social and political control.

Gus Hosein is a visiting fellow in the information systems group at LSE. He is also a senior fellow at Privacy International and an advisor to the American Civil Liberties Union project on technology and liberties. He specializes on privacy, the interplay between technology, society and civil liberties. His early research was in technology, policy, and regulatory change. Previous fellowships focus on international cooperation in criminal matters. His current research deals with anti-terrorism policies, civil liberties, privacy, and international policy dynamics. He is an adviser to non-governmental organizations in the U.S. and Europe and has consulted for a variety of governmental institutions.

So without further ado. (Applause.)

PANEL 1

>>SIMON DAVIES

Thank you, Naomi. Thank you to the FTC for the opportunity to set the scene for this conference. My name's Simon Davies. This is my colleague Gus Hosein. The Chairman described us as gentlemen. And I'll explain why that's not necessarily the case.

This is an important moment in the establishment of identity policy in the United States and, therefore, an important moment globally. Have no doubt that even though the primary driver today is identity theft, the reality is we are, of course, setting foot on the establishment of a national identity policy that will have ramifications that go way beyond the pursuit of solutions for identity theft.

In every country where we've been involved and every country we've studied, identity policy at a national level started with one simple, clean, pure objective and ends up cutting across the entire private/public/personal spectrum. It's the nature of the universe. It just so happens that in this country, identity theft is the core driver. In Britain, it was counter-terrorism. In Australia, it was tax avoidance. So, you know, but it all comes to the same thing, ultimately, we're heading toward an integrated national policy, for better or worse. Our job in the short time we have is to try and establish why this is necessary and why it is not necessarily bad.

I want to just put it on record that even though we do work with government – we, for instance, just recently completed advisory work to the United Kingdom treasury on this subject — we are reviled by a number of governments because we've actually stopped identity card systems because they were bad. Because they didn't put the citizen at the center. Because they intruded on privacy to an unnecessary extent. Because they were costly, cumbersome, and, frankly, that they wouldn't achieve their objectives.

That's why I say that we are not necessarily gentlemen to some governments in the world. In fact, for the past three years, we have fought the United Kingdom governments over its original identity card proposal, provoking a celebrated battle between the Prime Minister, the Home Secretary and ourselves in a very public arena. A lot of name-calling from their side. And we were as civilized as possible, but, in a very systematic way over those years established

through the London School of Economics and through hundreds of organizations and individuals, that the government was wrong. And I'm glad to say that after three years and something like $120 million of public money, they have now agreed with us. (Laughter.)

Which is why what we want to focus on is process. What you will see over the next two days is a showcase of ideas, of technologies, of initiatives. And I would say don't treat this as a competition at this early stage. It's not. Take a look at the process. Because that is the one driving force which will determine the success or the destruction of a good national initiative. In every country where identity has been successful and applauded by citizens and even by privacy groups, process has been the single most important element in every decision you make. In everything that you determine, you consider the way that you go about the process.

We call it the 5 Ds. You see it in the paper that Naomi mentioned. It's not just the question of saying we've got to have it for the sake of appearances or the noble objectives that we want to set out, we want to have an identity policy come what may. You end up with a situation, I don't want to be begrudging to our hosts here, but you end up with a situation like we have out here with the identity requirement at the front desk. Which is — yes, there is an edict from the Federal Government. There is an edict that has established as almost a truism that we have to improve security in federal buildings. But, honestly, I can go to Kinko's and get a picture of a dog with my name on it and it will be totally acceptable because the box can be ticked.

Let's say that we wanted to establish an identity for this building, an identity policy. It would involve a process that will be long, it will be consultative, it will be integrated and what we would end up with is a system that actually works. It functions so that all stakeholders benefit. Of course, I'm not singling out the FTC here. I got the DHS last month. I don't carry identity for this very reason. I want to see what the effect is if I don't have identity. In the end, I just walk through because it was just too much trouble, frankly, to deal with the identity requirement. So I think at a national level what we're dealing with is something that, at this building level, is as patently obvious as a series of challenges and processes that needs to be gone through.

Now, this is complex. And as I say, we are privacy advocates first and foremost. And privacy is going to be one of the key issues that you deal with. In fact, it's the killer aspect. Gus will talk shortly about the political risks associated with identity policy. And of course, the political rewards — and by political, of course, I'm talking the whole domain. And as privacy advocates, I'd say that it is not necessarily incompatible to have integrated national identity infrastructure that achieves core objectives and also have a privacy-friendly, citizen-centered system.

We have seen it. We have seen it throughout the world. Unfortunately, what you end up with, as we discovered in the United Kingdom before they saw the light, is a series of political objectives mapping out the appearance of a consultation and a process, but no actual structured approach to the problem. You end up with a disconnect between the objectives that you have— the needs that you have at a political level or at a national level— and the outcomes. There is a

huge gulf between the two.

And we take just some of these complex issues—technology, the application of technology, the interface with the individual, how do you get the take-up, for example, how do you get trust. The one thing that we can guarantee you, and what we want to discuss as we move through this conference, is the idea that if you have adequate the first D—discourse—at the government level, at a key stakeholder level, you move through to the dialogue and the deliberation with the public at large.

If you have a decision-making process which is structured, accountable, transparent, you move to a design process that loops back constantly to make sure that your technology meets your objectives, that meets all the criteria, and then finally a delivery which has in mind the bottom line. Does this work? Will people accept it? Does it function according to specifications? Can it deliver the objectives that were set out for it? In the paper we talk about these 5 Ds. How in every successful implementation of identity across the world, those 5 Ds have been observed. They're integrated, they loop back on themselves, and it seems very painful, I know, but there is a blueprint in everything you hear in the next two days.

If you can imagine—you will have in your own mind perceptions and questions. If you could then say, well how would we implement a process to make a decision about whether this is the best approach, whether this is the best technology, whether this is the right time frame or application, then I think success at every level is possible.

And I would argue that we have this extraordinary opportunity in this country for the U.S. to lead the world in responsible, privacy-friendly, citizen-centered identity that is applauded, that is integrated, that works for the government, for the people, for corporate America, which doesn't have the downsides of so many identity policies around the world, but which actually does achieve the objectives. And believe me, you'll find, you wait, it'll be like dogs to the dinner bowl very soon.

Every government department will come up with an objective for identity policy. All the corporate sectors will come up with an objective, with a goal. I will guarantee you that within three months there will be at least thirty clear objectives and goals set out and agreed broadly. What an opportunity to bring those together and to create an outcome that works for everybody. And that's why I say we want to focus on the risks, so you don't fall into the trap that governments like Britain did— and the process—so you can learn the best from other countries.

Now, at this point I should throw it to Gus before I consume more of our time. We just want to keep this informal and you can see how informal it is, or unstructured.

>>GUS HOSEIN

I like how Simon tries to sound principled in not carrying around ID, but one of the reasons is he's a menace on the roads so they refuse to give him a license for a good reason. I'm here to talk about the risks.

Simon pointed out all the great opportunities, I think, but here I'll talk about the risks. And these are the variety of risks. I'll just briefly go through my component of the presentation. So at first it's a political risk. I think when a process begins where they decide, they—the government or departments—decide we need to establish an identity policy, there is general agreement. Everybody says yeah, that makes complete sense.

So when, for example, in the United Kingdom identity cards were introduced as a concept after 9/11, public support was 80 percent saying, of course, we need identity cards. They haven't had identity cards since the Second World War. They say okay, things have changed. Times have changed. So let's actually move forward.

But it's actually a very costly policy politically because as people learn more about these policies—and I've seen this in every policy situation around the world—as they learn more about the policy, the support essentially drops. And now support is down to 50 percent for the identity card. That's six years later, but 50 percent. And when you deal with a policy that affects the entire population, 50 percent support is actually disastrous.

Similarly, in Canada when they introduced the idea of identity cards back in 2002, support was about 75 percent. And then it dropped down 25 percent, and it became untenable, and they had to move on to another policy.

A year and a half after the government managed to get their identity cards act through parliament, Tony Blair did admit that, "it is to me at least almost incredible that the proposal to introduce an identity register in the UK should be so extraordinarily controversial, but it is," he finally admitted. It took a lot of hard work to teach him that lesson, but he realized it is.

It might seem inevitable. It might seem to be a great idea, but as time goes on, it becomes very difficult. Actually, in the United Kingdom, it emerged — it eventually became a constitutional crisis where the upper chamber, the House of Lords, unelected House of Lords, was opposing ID cards, and the elected chamber, being the House of Commons, was promoting ID cards, and it came to an impasse. That's how difficult it actually becomes despite the fact you have 80 percent support to begin with.

The next challenge is drivers. We all agree, as Simon said, it's a great idea. We can come up with 30 reasons immediately why we need to have an identity policy, but we usually don't understand the drivers as well as we should. We think, okay, terrorism. That was the first reason for ID cards in the United Kingdom. As time went on, they realized well, actually, terrorism is not exactly a good reason to implement ID cards.

We need to create a movement around ID cards that's more consumer-oriented. So they then moved to identity theft. Identity theft is a very difficult beast. And it's harder to say—it's easy to say identity theft is of this proportion. But it's hard to say that these solutions that we're offering will do anything to actually reduce the severity of identity theft. And we've seen situations arise in the United Kingdom and the United States around these ideas.

So for instance when the government in the United Kingdom fell back on the idea that we need an ID card in order to combat identity theft, they said, well, identity theft cost the UK 1.7 billion pounds per year. The general public responded, well, that sounds like bogus data. They said we don't believe this. We believe that you're introducing this 1.7 billion pound figure just to get your identity cards through parliament, and that was, in fact, true. And so it decreased public confidence and had political ramifications, so on and so forth.

And there was an article recently in the *New York Times* about how there's scant evidence of voter fraud despite the fact that a lot of identity policy initiatives in the United States are around the issue of voter fraud. I'm not saying voter fraud is not a problem. I'm not saying identity policies will help solve that, but we need to really understand the nature of the problem that we're trying to solve before we move forward on grand designs.

The next problem is, well, do we actually have feasible goals? Can we actually develop a solution to the problems that we've actually identified? After the government managed to get their identity cards out through in the United Kingdom, they had the great challenge of actually having to build it. That's a challenge that they're still dealing with all this time later. And then leaks continue to come out of the government saying, as we see in this article here, saying that the scheme is doomed to fail. That's not advocates saying that. That's internal government reports saying we have all this ambition. We had all these political promises we made. And now we actually have to build this system and it's actually not as easy as we first imagined.

Next, the effective design choices. Are we actually solving the problem that we went out to solve by implementing the scheme that we're implementing? In the UK, government said we want to solve identity theft. We had a number of industry officials stepping forward saying well, actually by creating this massively centralized system where we take all the fingerprints of everybody in the United Kingdom and put them in one single database, you might actually be making identity fraud a larger problem.

In the United States, we encountered this situation with the Biometric Task Force where originally they said, we need to put RFID into the passports in order to enable secure border and travel around the world because of international standards. And then they realized that the actual RFID chip needed to be secured. It took them a while to realize that. But when they did, they had to go back to the drawing board because they realized that you could make the data less secure when you use RFID.

So again the effectiveness of the design choices need to be linked back to the political risk because when people catch on to—hold on, we were promised all these great things and what the government is actually providing is actually quite dangerous—there are political ramifications as a result.

Then there's the 'inevitable costs' argument. People who oppose national ID policy and national ID cards usually fall immediately on civil liberties and then onto costs. We're not here to say that the costs are the most important issue, but costs naturally, almost inevitably, arise in

the debates around identity policy.

These policies are highly complex. They involve advanced technologies, and as a result, involve serious costs. When the United Kingdom government first introduced ID cards as a concept, they said, oh look, this won't cost that much. It'll be 1.3 billion pounds, which was, at the current exchange rate, about 3 billion U.S. dollars over a 10-year period. That's what they promised. Only that much over a 10-year period. Within months they revised it to 3.8 billion pounds. And within months after that it was 5.8 billion pounds.

When the London School of Economics did an assessment of the government's plan for the identity cards act we actually found that when the government was speaking about 5.8 billion pounds, they were only talking about the costs to that one department, the Home Office. Not the Department of Justice. They weren't talking about how much it would cost the drivers licensing organization. They weren't talking about how much it would cost the Work and Pensions departments and the Health departments and so on and so forth. They were only budgeting for themselves. And it becomes very, very expensive.

In our estimates, we predicted a cost of about three times as much. And the government was very angry at us and started calling Simon particularly a lot of bad names, which is quite easy to do so. Eventually they realized, in fact, it is actually true. It is going to cost more. And when the costs go up, there are political ramifications.

Again, it returns back to the political. People in the United Kingdom now say maybe there's a bit of a point behind identity cards, but the costs are ridiculous. And this cost idea is not going to go away. As this scheme gets implemented, the costs are going to be realized more and more and the global support will continue to drop.

So we have seen situations in the United States where the cost argument just either comes up through studies or just in political debate. So I don't think any of these stories are a surprise to anybody. The first being the anti-terrorism identification program for workers and the second being the cost of Real ID becoming a controversy in the United States.

Who governs and owns the policies, and thus risk? In the United Kingdom, the government was adamant that the policy would belong to the Home Office. That is the Department of Justice equivalent. And so as a result, the system of design was very much law enforcement-oriented. It involved a collection of all 10 fingerprints, two iris scans, and a facial scan of every single person in the United Kingdom. Actually it is the most technologically advanced, and some would say civil liberties-hazardous, scheme around the world because most other governments with ID policies—national ID policies in particular—these are administered through other government departments, ones that are more citizen-focused or tax-focused. And so when you have schemes developed by these other government departments, the actual technological schemes that arise are very different in the end.

And so in the United Kingdom, people caught on eventually, got a hold on, this scheme is being run by the Home Office. While we agree that an identity card is a good idea, that it is

being run by the Home Office, that means they want to fingerprint every single individual. My mom's going to get fingerprinted. My grandma's going to get fingerprinted. Everyone in my family is going to get fingerprinted. And as a result, political risks arise all over again. It matters who owns it and who designs it. There is a very strong link between those two.

And then inevitably we come to the final risk that we've identified. That is privacy. And I can't and I won't harp on about privacy too much because I think everybody really understands that this is really — this is the battleground right here about privacy. This is a transformation of the relationship between the citizen and the state when you introduce a new identity policy. That language emerged in every single debate around the world about identity cards and identity policy — a transformation between the relationship between the individual and the state.

Simon was saying that you can create an identity policy that's citizen-centered. But you can also create an identity policy that puts the citizen at the center of a massive surveillance infrastructure where you have every government department, even the private sector, actually, looking in on the individual and able to track their movements and transactions and so on and so forth. It's very dangerous.

Yet it's easy to get this right. It can be done right. And we have seen successful policies around the world where they have been implemented in a way that has promoted privacy. But we have seen far too many, and particularly in the United Kingdom, we have seen far too many policies that the main goal was to actually put the individual at the center of a surveillance infrastructure. And as a result—and again with the same with all the other risks, it comes back to the political. Support drops further as people realize this.

I guarantee you the first day that the registration centers open up in the United Kingdom—this is what they actually called them—opens up new offices across the country to have people come in and get registered. That is you get interviewed, you get asked 30 questions about yourself, and then get fingerprinted and iris scanned, then people, the support will drop further and further. And I will pass it back to Simon to close off.

>>SIMON DAVIES

Thanks, Gus. I just wanted to loop back to the process issue given everything that Gus has said with sharp, the jagged, the bloodied edges to identity policy which you want to try and avoid. Remember the 5 Ds I talked of before. I think in, sort of, going through this deliberation, this process, it's absolutely central, again taking a look at the global experience, that you isolate what it is you genuinely and reasonably want to achieve.

Given what I said before, I hope—I pray this doesn't happen—that this becomes like a sieve which just goes across the country permeating everybody's ambitions, that you can actually nail it to a series of quantifiable goals. These are the targets, this is what you want out of the identity system.

In this first process, this first phase of the process, which is this discourse followed by the

deliberation, it is really crucial that you identify — this is where this workshop is important – identify what it is you actually want to achieve and what you think reasonably can be achieved. You will hear a lot about a lot of technologies, some of which are almost unfathomable, impenetrable in their complexity. But that's the nature of the beast. We already have those unfathomable technologies that are actually out there at the moment and serving the citizen very well. But ask yourself what it is that you actually want these technologies to achieve. If you can do that, if you can nail that down, quantify it, ring and fence it, then you are on the first step to establishing a national policy that can actually work.

What we have discovered in countries across the world is that this becomes like a sort of smorgasbord. Identity policy is a smorgasbord. It offers something to everybody. And again it's like checking boxes. You have a problem with perimeter security. You have a problem with national security. You have a problem momentarily with the Canadians coming across here and using the health system, whatever it might be. That was a hypothetical, by the way. (Laughter.) Or does it go the other way? I'm not sure.

For the moment in time, don't allow a situation where you can just tick a box and say yeah, it can do that. It can solve that. The one hope that we both have is at the end of this workshop, what you can do is establish not just what is a reasonable set of parameters for national policy that can solve a proportion of identity theft, but also nail all of these other needs that you have as a society and also get the policy process right so that you then integrate that into this five-stage line that will take you finally to your deliverable, which is your design and your delivery.

I would guess that that's where we stand. I'm not particularly – I think I speak for Gus here, too—not particularly concerned about what technology you used, because ultimately the credibility and the support for the scheme will stand or fall on whether you can deliver a system which is functional and which is flexible.

This is another problem if you look at countries like France, for example, there were two approaches France could take, two approaches it did take. You could take the punitive, structured, sort of rigid approach, quite fragile, which came from sort of the law enforcement elements of France. Or you could take the more commercial route, which is to say look, this is a work in progress. Identity is a work in progress. It is an evolving beast. It needs to constantly change and adapt to peoples need and to the needs of government and private sector. It has to constantly adapt to increasing sensitivities over privacy and security.

So there are all sorts of opportunities there to take a look at the international arena and say okay, let's get this right the first time because you won't get a second shot at this. Once you implement national identity policy, that's it. There is no going back. You won't get a second chance for a rethink, which is why today's announcement is absolutely central—at lunchtime. It will sensitize people to the needs to treat this as a priority, to treat identity policy as a priority that can actually solve a number of domains.

Anything more to add, Gus, before we can move on to questions, if there are any? This is

why I don't have a driver's license because I'm short sighted, which also means I can't do an iris scan, which is good.

>>AUDIENCE MEMBER

About five times you've mentioned countries that have done it right. Do you want to give us three or four names of countries that have done the right thing and can you tell us why?

>>SIMON DAVIES

Sure. Well I think what you got here – well, we haven't got a single country that got every aspect right. Not every aspect because that would be asking too much. But if you take a look, for example, at the emerging Australian identity policy. The Attorney General of Australia asked to meet us about, what? Six months ago now? Because this is a very hot political issue. In fact, 20 years ago, I led a campaign which destroyed the first Australian ID card proposal. They were very aware that they needed to learn lessons since the government nearly fell on the basis of that campaign.

They've actually been quite transparent and quite open with people. Their process has been not flawless but pretty close. They have, for example, realized the sensitivities of individuals to the ownership question. Who owns the data? Who owns your identity? They have actually given the identity token to the individual. You own it. So the control is very much—it is partly a perception thing—but has moved to the individual away from the state. So I would urge you to take a look at the Australian policy. I think that is pretty close.

I think Estonia.

>>GUS HOSEIN

The French and the Germans have actually taken interesting approaches. It's important to note that both France and Germany established their identity cards under non-democratic rule, but they still managed to develop identity policy that is far more democratic.

So, for instance, the Germans have a policy, implemented after 9/11 actually, that barred the creation of biometric databases. So any biometric authentication that takes place is 1 to 1 between the token and the individual, no centralized databases. So technically the UK scheme would be illegal in Germany.

The French government had two policies. One was pushed by the law enforcement department that said we must create a punitive scheme that involves centralization of biometrics and the creation of a new national ID number. The other government department that was more geared towards internal reform said, we do need a new identity policy but we don't need a new identification number because that would force every government department and every private sector company to have to redesign their system to deal with a new unique identifier. So they said why don't we create a type of wallet where it's a card that can contain all the unique

identifiers that individual has for every government department. So again the individual gets to have control over which identifiers are in place there.

So when they go to get their health services, they use the unique identifier as issued by the health department and the same for when they get their pensions, and so on and so forth. We have also seen a more advanced form of that policy emerge in British Columbia from the Ministry of Health, which is creating a user-focused identity scheme where I get issued with an online identity. And if I want to link that online identity with my driver's license, I can do that. And I can also link it to my passport if I want to. But I don't have to. It's not mandatory. So you can have a simple, relatively, quite simplistic identity for online authentication for getting access to healthcare services, but you can actually fortify it with linkages to other identity infrastructures. But it's all, again, up to the individual to do that. There's no punitive or compliance-based policy in order to enforce that.

>>SIMON DAVIES

Could I just add one thing, though, to what you said there? It's not necessarily the case that you need something to be added to the equation like an identity system or an identity card or a register or a biometric. It might just be—I hope this is being addressed at this conference at some length—that you actually need to take something away that is causing a problem. I mean, we take a look at the Social Security number here. We have 20 years now been aghast that it seems to be this beast out of control.

You could, for instance, create invisibility of the SSN through a token. Then add a credential, which could be validated against the individual, and if you want to tackle identity theft of course. So you're not loading some onerous requirement over the population. You are taking away something that is perhaps doing active damage, for example, in the domain of identity theft.

So I think there's two hemispheres to this equation. The SSN is certainly a key, in our view, and some real focus on that over the coming months would I think be very beneficial.

>>AUDIENCE MEMBER

Could I ask you to comment on and perhaps amplify the distinction between identity and the system for tokens that requires validation? I think you have commented on that, but I have seen that as one of the fundamental issues in the United States as we look at [inaudible] of Social Security. Perhaps you might comment on what is the distinction between those two elements and how those play out.

>>SIMON DAVIES

Gus, do you want to do it?

>>GUS HOSEIN

No, you go right ahead.

>>SIMON DAVIES

Well this is the distinction between tokens, identity, verification, authentication. The terminology is actually crucial.

Often what we talk about when we talk about identification is in fact just verification or authentication. We've been dealing with this, in fact we've been talking a lot to the UK government over this. How do you actually have minimal identification and actually move the authentication as your primary source of validation, if you like? I don't think any country wants a top-heavy system where every time you want to conduct a transaction, you have to identify yourself.

Now if, for example, you were to say, you get any number of examples around the world—biometrics, you're ultimately going to have to deal with biometrics, fingerprinting, iris scanning, you are going to have to deal with this front on. We have this view of biometrics. Be very careful, because as you know, biometrics is an emerging technology. It's constantly changing. It's under a considerable sort of weight or challenge.

But if you were to, for example, say to the citizen you are in control of the verification process because you can choose whichever biometric you want to place on a token, we will validate the token through, let's say, a government private certificate so that you know the token is genuine, whatever that token is. The citizen can then either—well, we say a PIN number is probably no particular use. But with a biometric, a single fingerprint that the citizen controls, that the citizen can revoke, you can possibly have a triangulation there which isn't privacy invasive but which actually does have a full validation spectrum to it.

That's the sort of thing hopefully that we'll be dealing with throughout the next two days, that type of technology. It's not that complex, though it probably is that costly in monetary terms.

>>GUS HOSEIN

I'm afraid we don't have any more time for any more questions. But Simon and I will be around for the rest of the workshop. And we're running two of the breakout sessions tomorrow. We're happy to discuss these ideas further and our discussion paper goes into much more detail about some of the issues that we raised today. So thank you for your attention.
(Applause.)

PANEL 2

>>NAOMI LEFKOVITZ

All right. We are going to move right on without taking any break to our second panel on identity management architecture. The moderator is Fred Schneider. He is a professor in the computer science department at Cornell University and he is the chief scientist for Team for Research in Ubiquitous Secure Technology or TRUST. He will introduce his panelists.

>>FRED SCHNEIDER

Good morning. Naomi said that I'm the chief scientist of this NSF science and technology center called TRUST. The thesis of TRUST is that trustworthiness problems are not technological. They're not policy-based but, rather, they have solutions only by combining technology and policy and it turns out in a fairly fine-grained way. So people who study only one or the other are not likely to solve the problem. And it's only if we work together that we will.

Identity theft could be our poster child, if you will. It turns out there are many problems like identity theft, though, so it's not the only one. The proximate problem is mistaken—a mistake that people make of confusing identifiers with authenticators. This is what happens with Social Security numbers, with credit cards and other things. None of that is technological. We've been making that mistake many years before computers became prevalent, before the web, before networking.

Perhaps what technology brings to bear on the picture is some clean definitions. Identity we can take as a set of attributes ranging from your name to your underwear size. Authentication we know to be done by something you know, like a secret, something you have, like a card or a token, something you are, like your fingerprints or your retinal scan. But this is primarily not a technological problem and the structure of the panel is intended to convey that.

So you see three people before you. You see five people on your program. I don't know what to make of that except Stefan Brands is flat on his back. He apparently pulled his back and isn't allowed to move. And Larry Ponemon seems to have come down with a stomach flu and thought he didn't want to inflict it on all of us, for which we perhaps should be grateful. Starting from my right is Andrew Patrick. No? Yes. Then Larry is missing. Then we've got Jim and finally Paul. And that's not quite the order we're going to speak.

What I'd like to do is address each of these panelists with a question and do one round of discussion that way. And then a second question. And I think that's going to leave us time, actually a fair number of minutes now that we have one slot open, for audience questions.

So let me start off by asking Andrew if you'd say a little bit about some of the properties you would expect an identification authentication system to have—to make it likely to be embraced.

>>ANDREW PATRICK

Thank you. Is this going to work? There we go. So one of the things that we're going to

be talking about a lot in the next two days is trust. And so I want to start off by talking a little bit about how people make trust decisions. In particular, I want to talk about consumers and trust. My background is in psychology, so I want to talk a little bit about psychology. How do people make trust decisions? And why is this important when we're talking about identification authentication?

So, when people make trust decisions, we know they do a couple things. They do make trust decisions based upon appearances. They do make trust decisions based on first impressions. But given enough time and given the importance of the situation, they will also do analysis. And they will make deliberate decisions on the basis of a number of characteristics presented to them.

At the risk of oversimplifying, let me mention three characteristics that people look for when making a trust decision, and, therefore, three characteristics that we have to consider when we talk about building authentication systems and we talk about how to design those authentication systems.

So the first one is competence. They make assessments about competence. They make assessments about the ability of a system or an organization to do whatever it is that they're set out to do. And so we are going to be talking about the competence of different types of systems, whether it's the nice people who greeted us at the door this morning and took our identification, or a biometric system, or a government program.

The second one is benevolence. Is this organization acting in a way that has my best interest in mind as a consumer? Is there something that is looking out for me? Or is this something that is the opposite, which is acting against my best interest?
And so they'll be looking for things that, from their perception, are benevolent.

And the third is integrity. Is this a system that holds together, that is impermeable to attacks and problems. So when we think about authentication systems, we have to think about these things: confidence, benevolence and integrity.

So let's think, for example, about authentication systems that are based on biometrics. I agree that we're going to start talking about biometrics at one point or another you can't avoid it. One of the areas that I've been doing the most thinking about is biometrics and the relationship between people, the subjects of the biometrics, the people who provide the biometric information and use those services based on biometrics, and their attitudes towards them.

So when people start thinking about biometrics and the competence, benevolence and integrity of biometrics, very quickly we get into problems. So, for example, there was a study done in 2005 by TRUSTe that showed that people really didn't think much about the possible integrity of a biometrics system.

So when asked, for example, what would they think about a biometric-based identification system, 71 percent thought that criminals would find some way to get around it

because that's what criminals do. So they weren't very confident about the integrity of the system. They also weren't very confident about the benevolence of an operator, or particularly a government operator, of a biometric system. So on this particular study, for example, 64 percent thought that the government would find some way to misuse the information, meaning using it in a way that wasn't initially intended or wasn't initially signed up for. And finally, 21 percent said they wouldn't trust the biometric technology.

We have other examples where we already know that certain kinds of authentication systems have issues about confidence, benevolence and integrity. When we talk about licensing systems, for example, and talk about the confidence, benevolence and integrity of the Department of Motor Vehicles, whether that's in the United States or Canada, it very quickly gets into lots of horror stories about the integrity and competence of those kinds of administrations, and certainly the Center for Democracy and Technology has been looking at case studies of integrity and fraud problems in the Department of Motor Vehicles.

The other things to think about when you're thinking about how users might relate to authentication systems are user confidence. What are the things that users are going to be looking for? They will be looking for reliability, which is performance that is accurate, quick, and consistent. They're going to be looking for usability, and in particular, they're going to be looking for transparency and feedback. When a system, for example, rejects them and they're not about to use their ATM card that is triggered with a biometric or their PIN, it is not enough just to say "access denied," but to provide some information. And some of the best biometric information systems that are out there, for example, even the ones that are simply controlling access to my laptop computer, for example, are getting better and better at providing feedback when it doesn't recognize my fingerprint and at least show me an image, for example, of what fingerprint it did get and some hints about why it might not be right. Maybe I scanned my finger too fast or missed the reader.

The other thing to think about is people are self-serving. People want to know what their interests are, and they want their interests to be taken care of. And so when we think about designing systems, we have to think about what is the direct benefit to the data subject. What is the direct benefit to the consumer? And we know that for security systems and for identification systems, the direct benefits that are of interest to them are convenience and improved services. It's often not security. Users are often not worried about security as their primary task. They're worried about security as their secondary task.

They're sitting down to access their laptop or do some banking. They're not primarily concerned with their security. It's a secondary concern and so what they're looking for is things like convenience and speed. And so those are the most attractive things for biometric systems. And security, people often don't understand the current security risks or understand what the enhanced security might be provided. So when we think about possible architectures or possible national policies, about authentications, we have to think about what is the direct benefit from the consumer's point of view? And does that match what the stated goals and policies are?

Privacy we're going to be talking about over and over. We continue to see evidence that

privacy concerns continue to be a hindrance when people are thinking about accepting these things. There was a recent study out by Deloitte, for example, that showed that there was little interest in the registered traveler program, which is a method for identifying frequent travelers, with 75 percent of the people citing privacy concerns, whatever that meant.

Finally, when people are making decisions, people develop mental models. They develop models about how they think systems work. And when you get mismatches between what an individual's mental model is about how a system works or how it behaves, or how it benefits them, and how it actually works, those are cases where you are going to run into problems.

So with biometric systems, for example, there is often a mismatch between how and where the biometric information is stored. So, for example, in the simple systems, people often assume that a biometric stores a raw image of the iris, or the finger, or the veins, or whatever system it happens to be, when, in fact, the system is storing some mathematical summary and storing it away in some encrypted form. Those are very, very different systems. They have very different performance characteristics, and very different privacy implications. And yet, there's a mismatch between the assumptions and the actual things, and better designs can make a better match and better acceptance.

There are simple systems versus advanced systems. Simple systems that are used to access desktop computers or pay for small purchases at a store are obviously systems that have little tamper resistance, little ability to detect spoofing and fraud, but are quite appropriate for the task. And yet we have other systems that appear to be very, very similar—driver identification systems, border-crossing systems that appear to be the same but, in fact, are much more robust and have much more integrity checks. So, again, we can have a mismatch between what the people think the mental model is about how these systems operate and what their characteristics are, and how they actually operate.

>>FRED SCHNEIDER

Thank you. We heard in the first session from Simon and Gus that we can expect a form of objective creep, or is that creepy objectives? Of objective creep, as various constituencies believe their needs are best served by an identification authentication system.

Jim, perhaps you can tell us something about those various kinds of goals people have for these systems and what kinds of properties the systems must have in order to satisfy these goals.

>>JIM HARPER

Thank you Fred, and thanks to the FTC for having me here and putting this all together. First, I just wanted to express some concern because I'm so used to playing skunk at the garden party, but I haven't gotten anything to work with in that respect because I thought Simon and Gus did lay out the issues very well, and they've obviously done a lot of good work on this in the UK that can translate well to what we're doing here in the US and what we're dealing with here

in the US.

Certainly I think that the place to start with identity infrastructure, identity management, what have you, is what purpose you're trying to serve. The matching of needs with ends, like Simon talked about. So what are you trying to do? And then design your system around that.

Unfortunately, we might have a lot of semantic fun on this panel and throughout the two days because I have a sort of hierarchy that I think of, and I use the word authentication much later in the process than other folks do. I think, in most transactions, and we really have to back away from the discrete problem that we're on right now of identity fraud and how we fix that. But back away from that and think about the sum total of what we're trying to do with modern systems and that is, to secure as necessary and to enable all kinds of different transactions and interactions.

And so I think that the first step in the process is to think in terms of authorization. Every transaction in society, whether it's economic or personal, can be considered as having a form of authorization. So for what are you authorizing is the first question. What is your organization going to do? What are you personally going to do? Then the second question is what credential do you need in order to go forward. In some cases the credential is age. In some cases the credential is height, at the amusement park, for example, the little thing that puts its hand up and says you have to be taller than this. Ability to pay or payment is very often the most important credential. And only sometimes is identity the most important credential.

Sometimes I like to illustrate the example of credential and the role of identity with the day I was getting on the circulator bus a couple of months ago heading home from work and just sitting there talking to the driver was a guy, and as I paid and turned to enter the bus, he said "Hey, how about a hug!" And I said "okay," gave him a quick little hug, proceeded down the bus, people looking at me like I was the crazy one, and it turns out that the credential necessary for a hug from me is absence of a bad smell. So not necessarily an invitation to you all, but there's an illustration of what kinds of things you need to authorize a transaction, in this case, a hug.

Sometimes it is identity, but it is identity a lot less often than we think it is. For example, the way our financial systems and money transfer systems are currently structured, authorization to issue a check, that is, to transfer money, that does require identity as found with a biometric in your signature. An ATM doesn't require identity. It's the combination of a card and a PIN code. So sometimes it's identity but a lot less often than we often think.

And I use the word authentication in terms of what level of proof you have of the credential. So what's the quality, like you would authenticate a painting. You may not have seen the painting when it was originally painted, but you know enough to be sure that it's the real painting, you go ahead with the transaction. Do you know enough to know that it's the person or a person with authority to do this thing, you go ahead. And the question is what combination of information, and sometimes identifiers, will prove the identity or other credential to a sufficient level to go forward.

So, how do we build this? Well, I think we probably don't. And what I mean by that is that we should let all the different systems that are out there blossom and flower. There are—when people open their wallets they're surprised when I ask them to recognize that the possession of that government-issued ID or driver's license isn't what makes them exist. Simon exists, despite not carrying that ID. But, in fact, the things we use to navigate society include our credit cards, business cards, ATM cards, all kinds of different things and all kinds of new things coming out.

The registered traveler program, you know, has a private issuer called the clear card. There are all kinds of different fobs and devices that are coming online. This is one that particularly interests me. It's a biometric fob. Well let's just see if I exist right now. I don't. All these different things are out there. They're being built and they provide a lot of opportunity for a system of systems. Microsoft Vista has a thing called CardSpace in it that is talked about as an identity metasystem because there are a variety of different technologies that will be used within it.

In this endless variety, I think, in the competition among all these different systems to serve all the different purposes we have when we transact—other rules for privacy. Privacy demands can be met. And I think the clear card in use in the register traveler program takes that into account and it takes a lot of work to ensure consumers of privacy. And I think the design of the system in terms of privacy assurance is pretty good because it will prove to the TSA that you're a member of the registered traveler program but it won't tell the TSA who you are. Now, the TSA doesn't quite get it so apparently they are requiring you to show government-issued ID in addition which is perfectly, perfectly senseless. But so it goes. We work our way forward.

I do think that in terms of policy the best thing to do is let all this stuff happen and the government policies can do at least one thing and that is not to bias the situation. We have many examples, I think, where governments demand government-issued ID by rote. In many states if you want to prove you're over 21, you're required to show government-issued ID, not something that proves you're 21. Getting away from those policies and getting to policies that will accept and embrace the blossoming of all kind of different identity and credentialing systems would be great. What was the question? I'd love to get back to it.

>>FRED SCHNEIDER

The properties of the goals that we'd like for a system? And the properties that would support those goals?

>>JIM HARPER

I think I've already talked enough and we can go back into all that stuff.

>>FRED SCHNEIDER

Okay, great. We all live in a sea of ID systems, even, Simon. He may not choose to participate, but you all have lots of credit cards in your wallet. You all log in to websites and each one asks for a password and I'm sure you give it a different password each time. And so a question, a natural question that arises is: Do we need another one? Do we need only one? And how do you reconcile all these ID systems?

So Paul, I thought maybe you would comment for us about the need for a new one or the ability to reconcile and unify the existing ones, and what are the challenges that we might have to confront in either unifying them or starting a brand new one?

>>PAUL TREVITHICK

Well, I agree with so much of what's been said I can be brief. First of all, we have got to work out from the consumer's perspective, and what are they faced with? Enormous inconvenience. Every new system that's put forward introduces another user interface, another card, another key fob. It is pretty much the opposite of convenient from the consumer's perspective, the citizen's perspective. The average person, it's said—I don't know the numbers—but exists in 1,000 different silos of database records out there, many of which you're not even aware are tracking information back to you.

So I'd say that if the goal is to make something adopted, IT has got to be convenient. Privacy and a lot of other stuff is critically important, of course. But if the system isn't convenient, it won't be used. And when I say the system, well this brings up the paradox. In fact, we don't need a new system. We need, to quote Microsoft's Kim Cameron, a metasystem or a framework. What we need is interoperability and consistent user experience. That's where we start. And I think what Microsoft has done with CardSpace is a great step forward and a good example in the online virtual space of what can be done.

In a sense, it's not a new system and it's attempting to be the bridging of existing systems. I'm not going to talk about a new biometric or any kind of credentialing or authentication system. There are already zillions of them. But if we want to attack this enormous complexity that the average person faces, we have to introduce a new abstraction.

We need something that's consistent and convenient. And in the online space we've been looking a lot at unifying around a card metaphor, a digital card that could represent so many different systems underneath the hood. Different identity protocols, different credentials, and different technologies. But unifying it, just like on a desktop, you know, we came up with the idea of folders and files. Now it's like, "of course." Well we're at the not quite "of course" state of identity. There is no common metaphor for how this stuff works.

So, in terms of the properties of the metasystem that we want to make, we want to, in my mind, embrace every possible technology that you can rather than impose some new system top down. We want it distributed in its design, and I think the way to deal with complexity is not trying to overlay a new über system with single identifiers, but in fact divide and conquer.

I think small is beautiful. I think that we should have as many different small authentication authorization contexts with as limited and small number of attributes, many of the times non-identifying.

And that introduces a paradox, because if we have more systems, aren't we going to make it less convenient? And that brings me back to the issue of not necessarily if we had a new metaphor, if we had a new abstraction. We can let 1,000 flowers bloom if we have a common abstraction and way of looking at them. And today we don't have that.

So why don't we try and do more with one rooted identity? Or let's just do one system. Because at least one system would be convenient. You only have one user interface. But everything we know about privacy policy trends in the opposite direction. It's almost impossible to make any rational statement about privacy policy when the contexts are too large. And then the only time that you can make a statement that anyone could understand about what should be shared or needs to be shared, the whole metric of appropriateness can only be evaluated in small contexts.

So I believe that if we start with the goal of moving towards convenience for the consumer, we will—this will be a driving function for the kinds of architectures and solutions that will really be adopted.

>>FRED SCHNEIDER

Thank you. I know that the press conference isn't until later but I'd like to take this opportunity to propose a new national ID system with hopes that the panel can critique it for us. So in my new national ID system, which bears no resemblance to anything you've seen in the newspapers, we'll assume that every individual has a unique identifier and that allows information to be aggregated and accessed under that identifier. And second there is no requirement that this unique identifier be used in all transactions or in any transactions.

So I'd like to understand what you folks feel is good and bad about this proposal and if you were tasked with implementing it and getting large-spread adoption, what would you suggest to me? Let me start with Andrew.

>>ANDREW PATRICK

Well whenever you're looking at proposals like this, you very quickly end up with a laundry list of things that you know really are requirements. Some of them we have already been introduced to. Some of them we'll be introduced to throughout the next couple of days.

But first of all if you're talking about a new identifier, how are those identifiers issued? A central issue becomes what are the foundation documents or the foundation information that's used in the creation of a new identifier? And how workable are those requirements? What happens if you don't have a birth certificate because it's been lost, stolen, damaged, cannot be recovered? What happens if you don't have proof of citizenship? What are the work-arounds?

What are the ways that systems can be flexible in creating identifiers?

The second thing gets back to my theme about shared understanding and shared models. What's the purpose and the role and the responsibilities of each of the players in an identification system? Both the users of the system, the subjects of the system, and the administrators of the system. And does everyone share the same understanding of what those roles and responsibilities are?

You say it will be voluntary, but how voluntary will it really be? And if some organization doesn't treat voluntary the way I do and requires that I show identification even though it's not absolutely necessary, then it's no longer voluntary and we seem to have a difference in how we view voluntary. And so we need to get this clearly established and shared up front.

Who holds the data? Who owns the data? Who has access to the data? Are there restrictions on the access? Is this data only for private sector use or public sector use, or both?

We've already talked a little bit about the centralized versus distributed nature of it. Distributed identification systems can be distributed among different agencies or systems. We've been introduced to the concept of systems of systems or families of systems. The information can be stored in a variety of different ways, from massive central databases to local, regional or application-specific databases, to something that's actually very, very local and stored only on a smart card or only on a key fob or only on my laptop computer. Those are very different systems.

So, for example, when looking at possible consumer acceptance of biometric systems and when people are asked: Would your acceptance of such a system change depending on where the information was stored and how it was stored? A Frost and Sullivan study in 2002, for example, found that market acceptance increased when systems were described that had biometrics stored on a smart card as opposed to some form of a database where the biometric information is very localized and restricted to a particular card. Studies in Europe have also found that acceptance of systems increases when you're talking about distributed user-controlled storage of biometrics as opposed to centralized storage.

You're building a system. What if something goes wrong? What are the legal remedies for me and for you if this system is misused? Do we have a clear and effective understanding of what the legal remedies are for misuse? And it might be criminal misuse but it might also be bureaucratic misuse?

What if I feel you have introduced a system and you're now using it in a way that I don't agree with, what are my options? What's my redress? Are there technical or legal measures to prevent data linking and function creep? You're introducing a national ID system with a particular set of characteristics, but what if you change those? Is there a legislated mandate that you're held to such that changes cannot go outside that mandate without legislated changes? Is there a way that these things can be restricted to specific purposes and not used for other

purposes?

And, finally, can we build systems that allow authentication, transactions, authorization while still enhancing privacy protections? And as we started to hear about, and we'll be hearing about later on, there are some technical means that are possible for separating out transactions and authorization and credentials from identity. And so we can look at systems that allow people to prove a credential without proving who they are or without even being asked who they are.

Thinking about biometrics, an area, for example, that I'm focused on, there are some new technologies that are being explored like cancelable biometrics, where biometrics can be tied to a particular purpose. The biometric information is transformed in some way such that it is only useful for that purpose. If the biometric information was ever disclosed in some improper way, it's useless in any other purpose.

And there's also new schemes being described about biometric encryption where biometric information is mathematically combined with encryption keys such that the only thing that the biometric information does is to create a key and then the biometric information is thrown away. And when someone goes to use the key, they use the biometric to unlock the key and then the biometric information is thrown away. So they get an effective set of keys without having any information about them permanently stored.

So there's interesting things that can be done with any kind of proposed system if one thinks widely about the variety of issues that might be involved in opportunities that are there.

>>FRED SCHNEIDER

Thank you. Jim?

>>JIM HARPER

I think Andrew got a lot of the right questions. I think they ultimately boil back to the question of who is the issuer? Because basically my first thought when you raised the hypothetical is—is it mandatory? And will it be mandatory? So a government issuer may not make it mandatory at the outset, but chances are given a long enough time horizon and usefulness, the thing could become mandatory and that would be concerning.

If it's not mandatory, then use of the identifier or the identification scheme, whatever it is, is subject to bargaining. I can present it sometimes and not present it other times based upon a variety of metrics or interests of mine including convenience, cost, and most importantly to me, privacy, which includes many, many different dimensions of data protection and then use limitations that Andrew talked about.

So you can have—national ID is a great rhetorical tool, the phrase, and I use it all the time to great effect. But you can have a national ID that's issued by a bank and it's really not all that concerning. I suppose it's more accurate to be concerned about a state ID or a nation-state

ID. But otherwise put it out there. If it's useful, if it works for consumers, if it satisfies all their dimensions of interest and need, go for it.

>>FRED SCHNEIDER

Thank you. Paul?

>>PAUL TREVITHICK

Well, there's this presumption that the only way you can correlate information is with one unique identifier. There's also this presumption that you're going to use this identifier all over the place. If you really look at what causes 95 percent of identity theft, it's that the information was hanging around in some database, some laptop, and it was stolen or lost or something. And that's because 95 percent of the time the information didn't need to be there.

So my answer will be: If you're going to build a new system, and it's going to be tied down to some unique identifier, maybe with biometrics, use it sparingly and then exchange it as quickly as possible for some other token, some other credential that isn't—doesn't have the unique identifier in it—and rely on auditing and other mechanisms to make the correlations. Because that way you don't have databases with this unique identifier all over kingdom come making it trivial to correlate identities unnecessarily. I mean, there are ways to blind the identifiers and use them in transactions most of the time.

And it's just this misperception that the only way we can build an identity system is to build an identifier system, when in fact most transactions can be done on attributes and roles and the actual identifier down to the carbon-based life form is not actually important for 95 percent of the transactions that are actually done.

I'm not saying that we don't need to root it into strongly authenticated identifiers. That was the presumption, so I can't even question the presumption of the question. But what we want to do is exchange it. Do a claims transformation. Exchange that for something else.

It's just like when you go into a hotel. They give you a room key. The room key doesn't identify you, it serves a limited purpose. And if I lost the key, it wouldn't tell who I was. Nevertheless, it's possible to trace back who I really am if there's a need to do that, if I committed a crime in my hotel room. So I think that notion of exchange, and exchange as quickly as possible off of the system that's uniquely identifying to something more appropriate for the context and the transactions at hand, the purpose at hand. That way 95 percent of the data will not contain the identifier, the global identifier.

>>JIM HARPER

I just want to mention that a notion that I keep coming back to in my head that Paul's answer reminded me of. I'm sure that people here in this room and certainly people that have spoken here understand well the sort of diversity of interactions and identities that people engage

in and adopt throughout their lives. But when I go and talk to people, particularly people in government about ID, they really do think that there's one identity that a person gets at birth and that's their identity through their entire lives. But we have dozens of different identities.

And I think Phil Windley, the former CIO of the state of Utah, expressed it very well when he pointed out that identity is a relationship. And we have many, many different identities. We adopt different identities for different purposes. And people have to understand that. That there isn't a single uniform identity. You do lots of things that may not be traceable back to your carbon-based life form. Many of them are, but with relatively tenuous links. And so it's much more diverse, much more complicated than just to think that there's a person, they have an identity, and if we just lock that down, we'll have a system.

>>FRED SCHNEIDER

So I think that Andrew brought this up. And I think that raises really the next question. And that has to do with centralization versus decentralization and distribution. Note there are a lot of people who believe that whereas I agree that identity is a set of attributes and it might not involve your name and your fingerprint, many people regard identity as a basis for doing the ultimate kind of enforcement, which is attributing actions to somebody you could prosecute in a court of law. And in that case you have to track things back.

But I wonder if each of you would comment on what you think the role of centralization and decentralization or distribution is and try to couch your comments in terms of what might be called the threat. People who work in security know that when you build a system, no system is secure and you start out with some threat model. Is this going to be secure against 13-year-old males with nothing to do on a Friday night playing with their PCs? Or nation-states who have nothing better to do than to try to break in.

So say something about what you think the role of centralization and decentralization is and how those things can be used to good effect and what you think the threat is. Shall we start with Andrew?

>>ANDREW PATRICK

Sure. But I'm going to talk about threat in a different way, and that is: What's the threat that's causing a proposal for centralization in the first place? And that is: Why would people consider that a central system, a central repository is necessary? And it gets back to the theme about truly understanding what it is that your identification system is being designed for before you go about and design it.

So let's think about situations where a central repository of information is needed. So you're looking at systems, for example, where you need to identify someone or you need to authenticate them across either a wide variety of physical locations or logical locations or services where you need to be able to say: This person is the same person or this authorization is the same authorization. And it turns out as some of my colleagues already said that those kinds

of situations are actually relatively limited.

And in a lot of situations, it really doesn't matter whether this person is the person who has credential X in one situation and credential Y in another. And so you have to consider those cases where a centralized system is absolutely necessary before you really think about why you would go about implementing them.

And so there are a couple of cases where you might want to worry about that. Obviously, criminal databases where you want to make sure that someone leaving a geographic area is—can no longer be found just because they move to another county or committed their next crime there.

Situations where you're trying to prevent duplicates. So duplicate enrollment, duplicate detection. Maybe situations where you need to do comparisons to make sure that someone doesn't claim a service in one location and then go next door and claim a service in another.

But for many systems, duplicates are not that much of a problem and so you really have to think about what kind of a service is it? Where if someone has two entitlements or two identities, is that really a problem? Again those kinds of systems are relatively rare. They do exist. They do exist for some government programs, for example.

But you have to think about what the threats are to the identification system before you can think about where the role of centralization might be.

>>JIM HARPER

There are so many different possibilities in terms of identity systems and different things you might centralize or disperse that it's hard to say that there's any hard and fast rule or anything close to it. My gut and my sense of things is that decentralized is better than centralized. Think of it in terms of trading different risks one for another.

And I think of a current example being the Real ID Act which broadly stated would centralize our identification systems and do some interesting risk tradeoff for arguable—and in my opinion disputable—national security benefits, you would get some risks to individuals in terms of identity fraud and in terms of mistreatment by the governments, whether it be the DMVs and certain employees or rather bad uses of the centralized identity system.

So it's a tradeoff between the interest of the nation and the interest of the individual citizens and residents. And centralization tends to favor the nation state where decentralization tends to favor the individual. So having now thought out loud about it, I'm really, really in favor decentralization. But there's no one standard that makes sense for every different system.

>>FRED SCHNEIDER

Paul?

>>PAUL TREVITHICK

I don't have anything to add. I agree.

>>FRED SCHNEIDER

So I heard, are centralized systems absolutely necessary? And decentralized is better than centralized and it favors the nation state. So I detect a distinct bias on the panel against centralization.

I want to explore that. I invite you to reflect on why you say that. When I put my technologist's hat on, then I ask myself what are the chances that one can compromise a given system? That is, get it to do something you want it to do. A centralized system provides one stop shopping. You compromise that and you win big time. But it also provides the opportunity for investments in scale. That is, I could build my Cheyenne mountain of investment opportunities, if you will, and invest greatly because the consequences are so significant.

Decentralization invites all the confusion and opportunities for compromise that noisy communication affords. It requires a significantly larger investment to be protected at the same level. Now we have 50 states building Cheyenne Mountain instead of one. And any one of them can break and we're in trouble, right? And it seems like it's more likely that it's going to lead to some of the confusion that is what admits identity theft today. That is, people who perpetrate this are counting on the fact that identity is fairly diffusely defined and there's no easy way to authenticate somebody.

So I understand your bias and I would like you defend it not using an emotional argument, which is easy because I think centralization is bad, appeals to many emotionally, but try to tease out either the technical or the legal reasons why your view is justified. Maybe we'll start with Paul since he has the most expertise in the centralized systems.

>>PAUL TREVITHICK

Well, the problem with centralization, which is sometimes necessary, is that it scales numerically but it does not scale in the complexity dimension. In working with the Defense Department on their 3.5 million issued HSBD-12 smart cards, do they have scale? Yep. Do they have the ability to scale into complex situations? Nope.

Because the kinds of identifiers, the root credentials that you can build that are long lived and you can afford, the investment in that kind of a thing has to be—by definition—static, very simple kinds of identifiers. And so just pure pragmatism, the world of identity, whether you look at it from the individual's perspective, I have many, many different identities, or you look at it from the systems' side, they have thousands and thousands of different transactional contexts which require different attributes about you, then the concept that there would be one central database that would hold all the attributes necessary for me to perform all those transactions is

simply not manageable. Who would update it? Who would be responsible for that? Never mind the threat surface you've just created for an attacker because you get into that Cheyenne Mountain and you've got everything.

So I don't think it's just emotionally "power to the people, power to the edge." I think that it's an issue of dealing with complexity. We can't make fine-grained authorization decisions unless we start considering context. What exact attributes do I really need in this circumstance for what purpose? And you find out that it varies. The attributes needed in one context are different from what's needed in another context.

So if you were to centralize it, you'd end up with thousands and thousands of attributes that would have to be kept track of, which doesn't work. So I believe that centralization should be used sparingly. There are obviously law enforcement reasons and many other reasons why you need to have identifiers that can correlate identities across contexts. We do understand that.

But architecturally, the default should be that new contexts don't—are decentralized, that stand on their own, that define their own local name spaces for identifiers, that define their own minimal set of attributes that will be necessary to perform the transactions in that particular context.

>>FRED SCHNEIDER

Jim, are you going to buy your way out of this question?

>>JIM HARPER

I may buy my way out of this question. First of all, I think maybe just an unintentional word choice. It's not necessarily bias to prefer decentralized to centralized. I think it's a product of careful thinking and prioritization of interests. Well, I'm just saying that it's not a matter of bias, but one of reason. It's not meant to be emotional, but rather meant to reflect values that we have in this country that we want to keep.

Maybe what you said, part of what you made the case for is the idea that central is more secure. If you did, I don't recall but—it sounded like it. I think it's important for people to understand that central is not necessarily more secure. It's sort of intuitive that it would be because then you can set a single standard and you could have the world's experts work on that one system. But it's important to flip security thinking.

And I think Bruce Schneider, who is a well known computer security guy whose thinking extends quite broadly to lots of different areas, is responsible for the notion that security really depends on the motivation of your opponent or your attacker. Which is why I bring out the money. This is a $1 bill. Many of you are familiar with it. This is a $20 bill. I hope for your sake you're familiar with it. In the time that the $20 bill has undergone at least two revisions in terms of its security against forgery, the $1 has gone through no revisions. And that's not because the printing office is lazy. It's because the $20 is profitable to forge and the $1 is not.

So it's not subject to attacks. You'd have to have 747s full of $1 bills in order to transfer the value that you do with $20s and $100s. So this is more vulnerable to attack so more effort has been put into securing it.

Think of identity systems the same way. Think of your wallet the same way. You disperse your assets among a wide variety of cards and systems and tokens, it's less profitable for your attacker to break any one of them so none of them are attacked. Not none of them. Certainly some of them will be attacked. But it's less valuable to do so.

So the criminals might just turn their efforts to lawful employment; a job at McDonald's. But a dispersion of that is as secure, if not more secure, than centralization of assets. So there is security argument for decentralization.

>>FRED SCHNEIDER

Let me point out to those of you who can think back to the days when you were young and there were books in the library. If we wanted to insure the long-term life of a given book, one model is just have one library and have it online and call it Google or the Library of Congress. And the other model is to have these hundreds of thousands of neighborhood libraries. And if you want to delete a book from existence, it's a lot harder to do it when it's in all those neighborhood libraries. So that's another example where distribution or dispersion gets you greater security. Andrew?

>>ANDREW PATRICK

Another aspect about the security question when talking about a centralized system is any kind of centralized system implies transmission. So it implies in some way getting data from the central repository to the point where it's being used. And so now not only are we talking about securing a data repository, but we're also talking about securing all of the steps along the way between that repository and its points of use. And as we've learned, I hope we've learned over the years that that kind of security for transmission is very, very difficult.

And the security for the end point, the end terminals is very, very difficult. And so not only is it security of the repository, but it's also security of the whole system. And it's also not just technical security but it's also human security.

When we're talking about centralized systems, we may be talking about systems that are accessed, accessible by hundreds, thousands, perhaps millions of different workers working on different aspects of that system. And so each one of those represents a vulnerability.

But with a centralized system, those vulnerabilities may be pooled together such that people with nefarious goals who are getting access to the system through one method or one purpose because it's centralized may be able to exploit that for a wide variety of purposes. So the security implications can quickly multiply because of the centralized nature and by

implication the multiple use of those things.

And the other, of course, is the classic privacy concerns, how a centralized system can be used to track privacy, sorry, to invade privacy by tracking transactions and tracking people's use. And the ability for centralized systems to be used for purposes that perhaps may creep in their scope over the course of time.

Again, distributed systems that are built for specific purposes with specific characteristics, particularly limited characteristics, can often have limited ability to be exposed to function creep whereas centralized systems that have multiple purposes and multiple amounts of information can be much more susceptible to function creep, to being used for purposes where it wasn't initially intended.

>>FRED SCHNEIDER

So what you heard actually were two different threads and I want to disentangle them and then I'll throw the floor open to questions. One was about implementation. Should you build a single computer system, if you will, or have many computer systems communicating?

And the other was about what gets implemented? Should you have a single identifier or families of identifiers?

The case of the dollar bill is the case where compromising a single identifier doesn't buy you that much is a reasonable case whether or not all those identifiers are stored in a single computer system or not. And the argument that one stop shopping by compromising a system applies to implementation.

So we do have tools to think about those things. And I'll invite you to introduce your vocabulary to the term trusted. You could ask yourself what is trusted about the system? What must it do to function the way it should? And the way you figure it out, what is trusted and for what, is to appreciate if what you're trusting for something disappoints you, you get screwed. If nothing happens when something disappoints you, then you aren't trusting it. So I've been asking all the questions. We do have time for questions from you folks, and I invite you to state your name, your affiliation, and direct your question to one or more of the panelists. Yes? And there's a microphone that will appear.

>>AUDIENCE MEMBER

Thanks. My name's Tom Oscherwitz and I'm with a company called ID Analytics. There's one concept you've been talking a little bit about at this panel which is obviously centralized versus distributed. I'd like to link that to another concept which is government versus the private sector. The private sector has a natural ability because of competition to lead to distributed identity regimes because a lot of different folks have different identities. Government, on the other hand, is often top down. I'd be curious what the panel would have to say in terms of the role of government, how the government can deal with centralized versus

distributed. It seems that centralized is a natural way for the government to go.

>>ANDREW PATRICK

I work for the Canadian government. And I wouldn't say that it's necessarily top down or cohesive or organized. In a lot of ways it works bottom up and quite in competition to each other. And as a result, there is often very different forms of identity that I have in my relationships to the various governments and government departments. And that might be a very good thing. So it doesn't necessarily mean that a government has to be emphasizing a centralized system. Government services and government programs could be very much decentralized, especially services that are much more regional in nature or much more specific in their focus where it's not necessary to have a single identifier for this government service versus that government service.

>>JIM HARPER

Cato Institute is a Washington, D.C. think tank that is dedicated to the principles of limited government, free markets, and peace. My answer would be obvious.
Think of identification in credentialing as an economic service, akin to payments or telecommunications or credit reporting. There's a lot of room for a lot of different things to happen to make that go. Like there are a lot of different kinds of telecommunications services. Like there are a lot of different payment systems that we use.

The government could adopt whatever identification or credentialing systems work. That's the most important thing. And that should be the role of government here. Where they need a credential, they should accept whatever system will satisfy that need rather than being both the provider of identity through, today, Departments of Motor Vehicles and the State Department, and the buyer of identity, in which case they often bias their own services or services of other components of governments. Being a participant in a market for identification and credentialing is where government can do the most good.

>>PAUL TREVITHICK

I'd like to underscore that. That's a great point. We need to decouple the credentialing from the use of those. In most systems, they're tied together. They're closed systems, right? You use the same organization that issues it checks it.

And this is actually what creates an enormous amount of cost because everyone, then, has to do their own credentialing. And so I think one of the benefits of a distributed system of systems is what Jim mentioned in that people can choose. Trust is always the relying party's local decision. I can choose what credentials will be acceptable to me. They don't have to be ones that my organization issued. And that's theoretically true today, but without sort of these metasystems and without this consistent framework, it's very difficult in practice to pull this off and so we keep reinventing the same thing, at enormous cost.

I believe that government doesn't have to be—first of all, everything that was said about government doesn't need to be top down is all true. But also it could be consuming credentials from the private sector. Why not? We just need to make this convenient, consistent, and interoperable. And that's the new challenge. We do know how to make great credentialing systems. We know how to build certificates. We know how to do the crypto. We know how to check them. But what we don't know how to do is to make them seamless, interoperable and convenient.

>>FRED SCHNEIDER

There are of course many examples of ID authentication systems from the private sector where centralization has reigned supreme. If you reflect back 30 years ago, you had a charge card for every store you frequented. Now Visa and MasterCard are the same thing and you might also have an American Express card. So centralization can occur in the private sector, as well, but I would echo Paul's comments that the enforcement dimension, what incentivizes people to participate in a system, is very different when it's legislated or when it's voluntary.

On the other hand, you all have different drivers' licenses at the moment and so that's an example of something that is not centralized.

Other questions? Yes, all the way on the edge.

>>AUDIENCE MEMBER

I'm John (inaudible). Technology is transient. As the fifth generation I could clearly testify to that. With the system out there on the edge and distributed systems, how do you deal with dynamic changes that have to go on in the system? Centralized systems are clearly much easier to change as time goes on. Distributed systems are much more different because, of course, you have to push it out to the edges where I am. I wonder if you could address some of the cost factors and some of the practicalities of the system evolving over time.

>>FRED SCHNEIDER

Did you want to address that to somebody in particular?

>>AUDIENCE MEMBER

No. I think all three of you guys are great, all four of you guys. It's an issue that I think is worth discussing.

>>JIM HARPER

I guess, though I don't think I'm most competent to answer, I'm most willing to speak. I

don't know if I buy the premise necessarily that a central or uniform system is easier to change because that system, once put to uses, will be resistant to change that could change the uses of the way the system has to work.

Think of the Internet, for example, where most of the intelligence is at the edge. And people use the network to do different things at the edge. I think that's what Paul is talking about in terms of a metasystem. So that it's actually a flexible, organic system that you need. It probably changes better, though quite messily compared to a centralized uniform system. But probably more quickly and for the better than a centralized system.

>>FRED SCHNEIDER

Anybody else? So in five generations of iPod, it hasn't changed that much. And that's the point. If you define the right things, people will replace components. And the Internet has lasted through many, many generations of computer hardware because the Internet is not about the hardware at the edges or even in sight. It's about a set of protocols. And the designers were visionary in deciding that the Internet would do very little and allow people to innovate at the edges. And if you look at how an identity system ought to work, it should also do very little but allow people to innovate at the edges.

I think the risk—and the reason many of you are here—is the risk that people will innovate. And they'll innovate in ways that are seen as impinging on privacy. And so that second part of the problem, and something we've never done successfully in technology, is building something that's general purpose, that is inherently limited in the innovation that it enables.

Other questions? We need a microphone over here. I'm sorry, sir. There and then you'll be next.

>>AUDIENCE MEMBER

My name is David Lefkovitz. My secondary credential is I'm a computer science professor at Temple University in Philadelphia. My primary credential is that I'm Naomi Lefkovitz's father.

And near the beginning, Paul used the word abstraction. And I think there's a useful model. Perhaps it gets a little technical. By the way, this is an observation. Not so much a question. In computer science, called object-oriented programming, in which, to simplify it, we have the notions of inheritance and isomorphism that give you a layered approach.

And we have the concepts of different kinds of access methods, things like public, private, shared, framed that can give different kinds of access at different levels of the system. We have things like rooted methods that allow people to come in and use actual programs to come in and use similar functionality but different kinds of attribute presentations. And so this could be a model, a technical model for what you're talking about. And it also can address—I

think would address an accommodation of the centralized and decentralized solutions that you're seeking. Obviously can't go into more detail here, but I think it is an interesting model.

>>FRED SCHNEIDER

Thank you.

>>PAUL TREVITHICK

I couldn't agree more. I think that when we talk about a framework, we're talking about an abstraction that's missing. And when we talk about the iPod staying the same and yet being different, that's because there's a line. The user experience and some things above that abstraction are the same. And below that abstraction there can be a lot of innovation. So this is exactly the kind of principle that we want to work towards.

After years and years of looking at these systems, we need to figure out what are the invariant principles that work here. And I think that gradually and slowly and usually only by mistakes we learn what the right level should be. What is the abstraction that we can do that allows the metasystem, the framework itself, to do as little as possible while allowing what's below that line to be replaced, swapped out, evolved independently. If there's a lesson from computer science, it is abstraction. And that's what we're grappling towards here.

In fact, it even ties back to the analogy of Visa. In a sense, that was an abstraction that allowed the banks—the banks do the work, right? They're the issuers. They do 90 X percent of the work of what goes on have and yet it's because of an abstraction that was introduced, there was a protocol, if you like, for how they should coordinate and how the clearing should be done that allowed it to be interoperable. All these different cards would work. I think it's a nice example of a kind of thing we would do well to invent the Visa, so to speak, of identity.

>>FRED SCHNEIDER

Thanks. So that question pending in the back.

>>AUDIENCE MEMBER

Thank you. My name is Tom (inaudible) and I write for a senior citizen's related newspaper. And this question probably is somewhat pedestrian compared to the other gentleman's very scientific question. People have—I have often seen myself as a person with a handful of credit cards in front of a gas pump trying to see which one works. And just recently in New York, they arrested a number of waiters because they were swiping the credit cards with a machine in their hand to get the numbers and farming out the numbers to those that would create the false cards.

What technologically do you see on the horizon that might prevent this in the future? Thank you.

>>FRED SCHNEIDER

Gentlemen?

>>ANDREW PATRICK

Specifically about cards and card fraud, obviously in the immediate future the thing that we're going to be looking at is chip in pin cards, which are cards that—I mean the immediate problem with card fraud is one of simply creating duplicate cards, creating false cards. And so the immediate solution is to create cards that are more and more difficult to forge, just as we've done with our money as it's evolved over the years, causing it to be more and more difficult to forge.

So the fact that a waiter can extract information off the magnetic strip of a card is all that he needs in order to forge that card is obviously a weak point and so one that's going to be addressed rather quickly.

Tying that card to an authentic user becomes the next step. And so to go beyond a simple pin to something that ties the card to someone more carefully is something that we're going to be looking at. But none of those are fool proof. All of them just make it more difficult in order to do the kinds of fraud that we're seeing today.

>>JIM HARPER

A practical thing for you to investigate is a product called the gratis card that has just been rolled out apparently. The PR push seems to be successful because I am now talking about it at an FTC event. But this is a competition to the traditional credit card that apparently is more resistant to credit card fraud of that type. I'm not sure how it works and I want to investigate it more carefully but I think it uses a pin code to prevent just swiping and calling of cards. So the gratis card is out there. It's one of many innovations coming up in this area that could help suppress credit card fraud and, of course, identity fraud.

>>PAUL TREVITHICK

Actually just when you thought you knew what I was going to say about decentralized is good, I actually think from the consumer's perspective, you're going to see centralization. You're going to see is—what I mean is you're going to see a consolidation to smarter, stronger authentication and fewer of them. And it won't be having all these key fobs and all these different cards. In fact, the key to convenience physically is to have as few devices as possible.

But that you can decouple the strong authentication from the digital identities and sensitive attributes that you're emanating out there. Those are completely separate things, right? Just because I have one—my vision of the future is I have a cell phone there. That's the end of

it. The cell phone has maybe a biometric that can be used in certain circumstances because sometimes you don't want to tie it to the person, right? You want to give your ATM card to your daughter to go run and get some money for you. It would be difficult if you had to send your finger along with it. (Laughter.)

So I actually envision the future is stronger and stronger authentication and fewer and fewer devices ultimately converging on some thing that you're already carrying, like a cell phone or something like that. And I think that's going to be more secure, more convenient. And it does, believe it or not, it does follow the principle of decentralization because only the user of that device is the one that knows the correlation, that knows all of the different sets of attributes, the multiple sets of attributes that are stored on the single and rooted in the single device.

>>FRED SCHNEIDER

Did you want to say something?

>>JIM HARPER

It's another sort of bigger picture thought that doesn't necessarily relate to the question or to Paul's comments. The interesting question of centralization versus decentralization. There will be systems that are decentralized in some respects and centralized in others. Of course you cited a good example of the private sector centralizing on a few credit card systems that are national in scope versus multiple different credit cards with multiple different providers.

And that brings me to recognize that fixing the identity system or creating a good identity system isn't going to solve all of the privacy concerns that we have because someone may well choose to identify themselves precisely the same way with every one with whom they transact. And then they've got privacy problems. And the credit card payment system we have today is a good efficient system, but it's also not very privacy protective. So I think there's room for there to be payment systems that are privacy protective and convenient. We don't have them yet. But there are centrifugal and centripetal forces that both can have play. It just depends on which thing you're prioritizing at a given time.

>>FRED SCHNEIDER

Right. So I'm going to slowly work my way across this way. So I guess in the back there.

>>AUDIENCE MEMBER

Hi. Mike Jones from Microsoft. Two of us sitting here had the same reaction to something you said, Andrew, so I want to push back on that. You said that one of the problems with central systems is that then you have to secure the transmission of the data to the end point.

And yet as Paul will attest, I go around the country where one of the key lines that I'll

give is that we as computer scientists know how to secure a strong connection between here and there that can't be spoofed, that can't have messages interjected, that you can't inspect. That's easy. That's cryptography and technology. The hard thing is securing the two feet between your screen and the person. Why do you think the transmission is hard? That's actually the one soft problem.

>>ANDREW PATRICK

Because I include those 2 feet. I think from a human point of view, and so I think about the transition from one set of eyes to another set of eyes. Although we may know how to do the cryptographic protection of the information on the trunks, we're not very good yet on protecting the information in the end devices, for example. Or in the human factors where we have that interface between the people and the technology that they're working with.

>>AUDIENCE MEMBER

But that property, the securing the last two feet, is actually independent of whether it's a decentralized system or a centralized system.

>>ANDREW PATRICK

Yes and no. A centralized system may have more eyes, more people involved, therefore more places to secure, and may have people at either end of the connection.

>>FRED SCHNEIDER

Okay. I think over here.

>>AUDIENCE MEMBER

Hi, my name's Denise and I'm with Privo. And I have a real life, day-to-day identity issue. Every day I wake up, I have to figure out how to help my clients obtain verifiable parental consent under the Children's Online Privacy Protection Act. So it requires me to give parents a way to sort of identity-proof who they are so that they can then process what information we can then send through our system to a client site.

So because of that area, I've been watching all the age verification issues that are coming up and the state AGs talking about passing new legislation that would force the centralized database of My Space of 130 million profiles to start to vet identity for the purpose of separating minors from adults.

So my question is: Do any of you on the panel see any way that the government may ever step up or individual states or someone that would an allow me as an individual to prove that I'm 42 and have an anonymous credential that says, I'm female, I'm 42, I don't need to prove to My Space any more than that to be let into the adult population and on the same hand

maybe school systems with a pass/fail and a child student ID being able to get something that says I'm 15, I'm a boy, let me in to the kids' section.

>>FRED SCHNEIDER

Denise, I don't believe you don't get flattered when they ask you to prove your age going into a bar.

>>AUDIENCE MEMBER

Thank you very much. Is that on the record? (Laughter.)

>>FRED SCHNEIDER

Comments from the panel?

>>JIM HARPER

Well, I've been watching this issue, though I haven't been very active on it. My colleague, Adam Thierer at the Progress and Freedom Foundation, focuses on this a lot. He's got a paper out and there are a couple of other papers that I think. Let's start at the beginning that child predation is important and awful when it happens, but it is not as big a problem as it's being assumed to be and the AGs are motivated not by a rational assessment of the problem but by politics.

Now, trying to verify ages of children requires you –

>>AUDIENCE MEMBER

Well, let's just start with adults because I've heard a lot of arguments about children.

>>JIM HARPER

Either way, you're either excluding someone from a population or including someone from a population. They're just the converse of the other. They're the same for these purposes.

It's probably a mistake to do it. You're probably creating more risk by relying on a system like that. Because then somebody who breaks the system, who is able to prove that they're 13 using their child's identifiers, they're home free. So if parents were to think that there is an age-verified space on the Internet that's safe for their children, they don't need to be involved anymore in protecting the child and teaching the child right from wrong. That's going to cause more harm than it's going to prevent harm. So it's a very, very bad idea in terms of security and it will hurt children if this kind of thing goes forward.

>>FRED SCHNEIDER

Question here.

>>AUDIENCE MEMBER

My name is Jim McCartney. I'm with the DOD Card Access Office. How do you see mutual authentication playing in this? For example you talked about one card with multiple identities saying, for example, who are you to ask me for that? And depending upon what that response is who I say I am.

>>PAUL TREVITHICK

I'm not sure I understood the question.

>>AUDIENCE MEMBER

For example, mutual authentication. Who are you to ask me for my identity? And based on that answer, I give a specific or different response. I may give one person my driver's license, one my SSN. How do you see that as playing in? Because that would be a huge part of saying who are you to ask me? From a consumer perspective, I want to know who is asking me and do you have the right to ask me that question?

>>PAUL TREVITHICK

Right, I wasn't—now I see the question, okay.

>>JIM HARPER

I'm going to start asking federal agencies for their birth certificates, that's what I'm going to do.

>>PAUL TREVITHICK

To chip away at that. One small thing that I do like where things are going is the concept that the relying party has to disclose more about what it is that they want, need, and why. And I think that's a change that's in a good direction.

In fact, it's a requirement for any kind of interoperability, right? Because if the relying parties have to be declarative and disclose what sets of clients they need, what kinds of tokens they're willing to accept, and who they trust and so on, if they can do that and advertise that, then we allow, we empower the consumer to have an agent that then does the matching that tries to find an appropriate identity.

So just a little part of your very much too hard question was that I like this concept of the relying parties having to advertise their policy. And not just for the transparency, but for the automation that that enables and the interoperability that that enables. Again, we're trying to make a more open system, right?

>>FRED SCHNEIDER

Let me point out that this mutual authentication problem is one that is actually with us now. I understand that our concern here is mostly with identifying, authenticating people. But if you ever visit a website, you probably want some assurance that it's your bank's website and not somebody else's website. And that's what phishing attacks are about.

And what you find is that computers are good at doing certain things. They are good at memorizing things and computing, and people are not so good at doing those things. That's why it's a hard problem for you to memorize all those passwords. So authentication problems involving people appear in two guises. One is authenticating people and that's what this card might be about, and the other is allowing people to authenticate sites.

Now, it might be a website, but it might be somebody else who is requesting an authentication credential. And we don't know very well how to do that. We do know people are good at some things that computers are not good at. And we haven't yet figured out a way to leverage that. You would expect maybe a person could recognize a phishy looking website. To take an example, all of you are good at recognizing dicey looking neighborhoods if I dropped you into the middle of them. That thing has developed. But you're not so good at recognizing dicey looking websites. There was just a study done at Microsoft that made it quite clear. And there are a number of other studies. But this is a very important question.

The good news is it seems to be independent of the problem technically of identifying humans I think from a policy and legislative point of view. It's not completely independent and it's something that we'll have to come to terms with.

Before I take another question, do you folks want to make any final comments? Because we're going to be out of time soon. No? Okay. So then we have time for one more question, perhaps. And it's right here.

>>AUDIENCE MEMBER

My name is John (inaudible) with Hampshire Research. I won't stand so I don't block your faces. Paul, I'd like to challenge you in particular, but maybe the rest of the panel, to come back to the definition of the term "identity" because it seems that the risk here is that it's conflated too often with human interactions with the system that there is, in fact, a real identity that we all possess. And the challenge of so many transactions is to be able to do this on an ad hoc basis, on a peer-to-peer basis.

One of the key challenges would be the sharing of electronic medical records. So we do

need a mechanism, many commercial, governmental, and other transactions to have absolute certainty of identity. And it seems that the real key for us at the beginning of this conference is to separate what really is identity from what are the attributes of human interactions with systems.

So let me just ask you to reflect upon that and maybe adjust your earlier definitional approach and try to embrace some frame where there is a meaning to identity that does come back down to the individual and our ability to identify that individual.

>>PAUL TREVITHICK

I have a peculiar way of thinking of it. I think of everything as being a set of contexts in which you have—people have manifestations of themselves which show up as a set of attributes. And, yes, there are special contexts like the carbon-based life form context where you can talk about identifying the body, the person's physical body. And there are contexts, obviously related to medical, especially, and many others, security, law enforcement, lots of other situations, where it is necessary to be able to identify a person as a dot in that context. But the reason I think of it this way is that if you just think of it as another context, then it forces you to think rationally about what the requirements are when you actually need to make that correlation. This anonymous identifier in this context can be tied back to this point in meet space if you like. And who is privileged to know that correlation? Actually taking your medical example, I think one of the key learnings is that anonymity and pseudonymity is absolutely vital in order to have functioning healthcare systems because people's information is so unbelievably sensitive in certain cases that the possibility that it was tied physically to their identifier has to be questioned to the utmost.

So it's actually interesting you started your question off definitionally. I try not to use the word "identity" actually when I speak. I have not found it a helpful word. It is so conflated and overloaded by different things. You know, am I talking about me? And so on. And what we find, as system designers, of all ironies, and this is nothing new. But over a 300 year philosophic tradition, it turns out that what you're so attached to, that your sense of spirit and so on and so on does not need to be modeled by this system. And, in fact, you exist only as relationships in various contexts. You're just a bunch of links from the point of view of everyone else, and from the point of view of every computer system that needs to be modeled. And there's nothing about you that can be specified that is context-free, other than you being these relationships.

So with that as the mental model I always use, I try actually not to use the word because of this overloading problem.

>>FRED SCHNEIDER

The nice thing about the medical records example is people don't seem to balk at biometrics as a basis of doing authentication in that sense. Ok, why don't we thank the panel? I think they made some very interesting observations.
(Applause.)

And I'll hand it back to Naomi.

>>NAOMI LEFKOVITZ

Thank you. We'll take a break now. We'll come back at 11:15.