PCAST Meeting - November 21, 2013

Welcome & Education Information Technology (EdIT) Letter report

>> John Holdren: I wonder if we could get going here. We're a couple of minutes behind, but not too far behind. Let me welcome the members of PCAST, the members of the OSTP leadership, and the PCAST secretariat from OSTP who are here and let me welcome the members of the wider science and technology community, who are joining us either in person or over the live streaming webcast, which is underway. We have as usual a full agenda. We'll be turning to it in just a moment. I just have one matter of celebration to note that's our PCAST member Mario Molina yesterday received from President Obama the Presidential Medal Of Freedom. I want to congratulate Mario. I believe with this award it can be safely said that there's no prizes left that Mario has not won, and therefore he can relax. Not likely. Eric, would you like to add any words of welcome.

>> Eric Lander: I would like to welcome the whole PCAST including our two new members of the PCAST. We're very excited to have Michael McQuade and Susan Graham who is joining us in PCAST and we just have a lot of things going on. We're going to hear about two very exciting and important reports. So thank you everyone, as always, for the hard work and for being here.

>> John Holdren: Let us turn straight to the business of the day and the first item on that agenda is for PCAST to discuss and approve the educational information technology MOOC focused letter report. Eric?

>> Eric Lander: Sure, the question of education in general, STEM education in particular, has been a topic that PCAST has been focused on since the beginning. We've had two extensive reports. The one about the K 12 education system, one about the early years of college, there on the screen right there. both of which made extensive recommendations across the board of STEM education. PCAST is also in that first report very aware of the growing role of technology in education, within STEM education but within all education. And so PCAST has set out on a path of studying and producing the series of letter reports on developments and opportunities for technology in education. And the first, and it's just one component, is the subject of MOOCs massively open online courses, which PCAST discussed, we've had a session on them. And at this point we'll be discussing a report, letter report, on MOOCs within this larger topic and then at later meetings we'll return to other topics under that heading of technology applied to education we'll turn to Jim Gates who will start us off on this report together with his co-chairs.

>> Jim Gates: Thank you Eric, as was mentioned this is a subject that our group has concentrated on from the very beginning. Of course, we inherit this interest from the president showing acute dedication looking at this range of domain space and issues and so we have been in fact looking at STEM Ed from the very beginning as a tool for access to the American dream as we look toward the next couple of decades. So in this role, we have done the two reports that are on the screen now. Now we're moving on to a next phase. This next phase is in fact a multi phased effort. What we plan to do is

to actually have an arc of reports, all looking at the issue of educational technology, education and information technology and how this new technology and these new platforms and these new techniques can be leveraged to improve the efficiency and the transmission of the knowledge, skills and expertise that the members of the American public will need in order to navigate successfully the trying and possibly disruptive changes in the economy that seem to be on the horizon. So the first -- so I want to talk about the arc and then we're going to be talking specifically about this current letter report and I'll turn that over to one of my colleagues. So the arc that we're thinking about looks as follows. The current report which we'll be turning over today for the consideration for the entire group to look at is really, although we talk about the shorthand being MOOCs, massive open online courses, and really what's going on here is looking at how information technology can be inculcated into this domain to increase the efficiency of what goes on. So I'm going to stop here, as I said, one of my colleagues will be talking in more detail about the letter report, which I think most of the members have seen. It's been in your briefing books and we're pretty near completion. Of course, as the usual sort of modification subject to discussion coming from the rest of the council. The next part however of our arc, we are very excited about and in fact the small group of us this morning got together to talk about it and it's on the whole issue of workforce training, re-skilling and adult education. In this new economic environment people are going to likely have several careers. The 30-year-long career at a single institution probably is a thing of the past. So how do we prepare our workforce to engage successfully in this environment. Retrain, re-skill several times so that in fact the American dream can still be realized. So in the second report we're going to be looking at this issue and in particular what might education IT bring to the table in dealing with this. We are starting to plan for a workshop where we're calling national experts from the various relevant parts of the economy. We'll be looking at skills development. We'll be looking at targeting sectors. What are the sectors of the economy where it looks like there's going to be growth and opportunity for employment. We're also going to be looking at the delivery sectors, mainly traditional four-year colleges, two-year colleges and perhaps other parts of the environment where the training re-skilling and certification will be taking place and how at the cross-cutting boundary of information technology can we get better at that. Skills assessment is going to be critical. How do we actually put metrics in place to measure the abilities people have to have the these jobs to align with the needs in the workforce, skills maintenance and upgrading is going to be a huge issue. Looks that perhaps the two-year colleges will play an increasing role play a major role there and for the future looks like there's great demand for that. The President has on a number of occasions spoken about this possibility. And then finally certification mechanisms, because the skills that we're talking about and the kinds of jobs that we're talking about are things that are at some level technical, but they may not require a full four-year program. They may not require that one sit in a classroom. It's something the whole notion of something I'll borrow a phrase from my colleague Craig Mundie technician nation, an idea about where high quality jobs will reside in the future so we'll be looking at that domain. That's the second report and finally our third report is looking at K through 12 at the cross cutting boundary of information technology. As Eric Lander mentioned in our introduction, if you look at our first report to prepare and aspire and in particular look at the sixth chapter of that report, you will find that it was very, very forward looking. In fact, if you go back and read that part of the report, you will find something that sounds like a description of MOOCs, and yet this was several years before the words were even invented. So we were very forward looking in that section of the report, anticipating the technological changes that would be out there. We'll return to a more focused way looking at K through 12 that's the arc we'll be doing. So at this point I'm going to turn the discussion over to my colleague Rick Levin, who is going to talk a bit about the first letter form report that's near completion and we'll be forwarding shortly we presume to the president. Rick, you have the floor.

>> Rick Levin: Thank you, Jim. So I first want to say that this area attracted a lot of interest within the PCAST, and in fact virtually half of the members participated in the drafting of this seven-page letter. So you can imagine. But I want to thank Craig Mundie, Dan Schrag, Chad Mirkin, Jim Gates, Mark Gorenberg, Shirley Jackson, Barbara Schaal, all who participated in the project and Susan Graham our newest member on her first day made substantive and significant edits, and it was very much a group effort. The President has expressed on several occasions concern about the rising cost of a four-year higher education and worries about the barriers to access that might be created by rising costs and has set the educational community on notice that that's an important concern of his. And preserving the American dream of upward mobility through education is something of paramount of importance to him and to us. So the advent of the massive open online course offers at least some hope that the rising costs of higher education at least in the instructional dimension, if not the residential and extracurricular dimension can be mitigated. And so we wanted to look at this issue, and it's, of course, the MOOcs have attracted a lot of attention over the last two years or so and they do hold considerable promise. Now in one respect MOOCs really aren't a brand new concept. That is to say we've had massive open online courses for some time. Going further back in history there were correspondence courses in the days of snail mail, the British Open University was a very large scale effort that reached lots of people through television. Many universities have offered online programs of particularly to employers like Stanford's engineering school for a long time. And within the last decade universities like University of California At Berkeley. MIT and Yale have put up open to the public for free entire videotapes of entire undergraduate courses just for free availability to anyone who wishes to view them. What's new, and there is something distinctively new, is that within the last few years, the combination of broader bandwidth and software innovation have really allowed this to be much more effective and scale so that there can be simultaneous synchronous interaction among literally tens or hundreds of thousands of students at one time taking a course. This was not possible five or six years ago. It's possible now. And the quality of the transmission with higher bandwidth, even compared to what some of the online efforts that I know my university was making just 10 years ago, massive improvement. So you really can produce a high quality visual experience and learning experience now at scale and that's new. Has important implications one for costs because you can educate lots of people with a smaller number of faculty that reduces costs but also potentially for quality. Because you can test students along the way and these new innovations do this. They do regular interactions. So it's not a talking head for 50 minutes but often broken up every ten minutes so that there's opportunities for quizzes and interaction so that the real time data can be collected, can be analyzed, can allow for mid course corrections and improvement of the instructional material, if you find that there are situations where students have difficulty with some of the questions. So there's a really great potential, not just for lowering costs, but actually improving the quality of educational materials and hopefully the learning outcomes. So it's this capacity to measure student comprehension in real time. I think that's a really novel and very promising feature. It also has of course big data aspect, we're operating at scale, and well maybe not big data but

data aspect of operating at scale and then allowing us a lot of information. There's a whole new industry that seems to be emerging to supply these courses where firms that have entered and varied from purely not for profit enterprises, sort of controlled by the educational institution, the the edex model started at MIT that form. And there's the model of the for profit institution that's cooperating with universities Cosara, and there's an example of a for profit institution that is working in part independently of universities. Udacity. So we're seeing a variety of organizational types in the field. It's really quite a fluid situation. There will undoubtedly be other entrants and it's a little hard to predict which way the future will go. Next slide. In one other dimension, it's interesting to explain how the MOOCs have many flavors in terms of the breadth of the offering and presumably the cost or tuition that will be charged to students. Down at the bottom of the pyramid we call plain vanilla MOOCs are what we see most of now, which is courses just out there. They're online, you can sign up and take them you don't have to pay them there's no certification. The next layer is to issue a certificate, some are providing certification of completion for a small charge. The next level would be to offer course credit. And where, for example, we're doing a couple of those at Yale now, where you can get credit for a particular course at a somewhat higher tuition level. And then there are those that are maybe not -- they're really quite focused MOOCs on developing skills or sets of skills or clusters of courses that might help develop one for vocation or particular kind of employment and finally whole degree programs that can be mounted and we've got experimentation in that space. There are concerns and caveats we mentioned in the letter and they are fairly widespread in some of the educational communities. First one, I think it's really important, it's really keys into one of our recommendations, this is in the very early stage of evolution. And there will be lots of learning, lots of failed experiments, we shouldn't think because one program turns out to be a failure that the whole exercise is doomed like any start-up industry there's going to be trial and error and successes and failures. A second concern expressed by lots of people in the educational community and we have to keep this in mind. MOOCs don't offer the whole experience that a four-year residentially based college can offer. They may prove to be superb in the mastery of content but they're as yet unproven in developing the critical thinking skills, the skills of argumentation and rebuttal that are so important in a fully educated person and the whole extracurricular experience that goes with a college education, maturation of the individual, opportunities to learn how to lead and be a teammate, how to cooperate on projects. It's not impossible that some of those skills can be taught online but we haven't gone very far to develop those characteristics as yet. And obviously there's all kinds of, we think about reducing costs, there are a lot of costs of higher education that would have to be borne anyways that are part of the cost of education. Students have to be housed, have to get medical care. They have to, often need counseling these are things that colleges provide bundled into the cost of college that of course would, won't be covered in a space. It's just early. This is evolving. There's a lot -- we have a lot to learn. But it's exciting. Going now to our recommendations, the first recommendation really builds on what I just said, and that is it's too early for the government to intervene and try to give direction to the specific types of courses that could be developed or the types of needs that should be met or the types of institutions that should provide them. We really feel strongly. It's a time to let, so the government should be a close observer of what's happening here but let market forces decide which innovation in online learning and teaching are best. The government has no direct control over accreditation that is done by regional bodies but those voluntary cooperative bodies that operate in various regions of the country to accredit educational institutions have many rules and restrictions about what should count for college credit. For example, they tend to get an accredited degree, colleges have to provide appropriate library resources, for example. Lots of things that maybe don't make any sense in the MOOC area where they would make perfect sense for residentially based colleges. To the extent the Department of Education has any, is listened to in this arena, it should be flexible and encouraging accrediting bodies to loosen up and gives them room for a real genuine innovation in this space and not insist that online providers necessarily supply all of the attributes that a residential university or college would provide. And then finally and probably most significant recommendation we're making I think is that there is going to be tremendous learning from this period of experimentation and this is where the government could be very valuable by supporting research on the effectiveness of these online technologies, educational technologies, and encourage the sharing of results on effective teaching and learning among the providers. We note that the government could do this by sponsored research programs, by having, expanding some of the existing grant programs to cover this area, and then encourage through conferences and meetings and creating a community of scholars in this area to help speed the learning, help speed the diffusion of the learning that will take place through development of online education. There will be some pressure, of course, from these proprietary companies to try to keep what they learn about their students private. But if the government has grant programs for university researchers to study this problem, there will be pressure from the universities on the online providers to open up the data. And we think that would be a good thing. So those are our recommendations. We think this is an exciting and promising development and we wanted to call the President's attention to it and make a few suggestions for support and we all look forward to the continuing phases of this educational IT initiative that Jim gates has been leading so ably. Thanks.

>> Eric Lander: Jim anything more you want to add there?

>> Jim Gates: One or two things I wanted to, as Rick did, mention a number of colleagues on PCAST joined on this one this one sort of fits into a sweet spot for the council as a whole. Council composed of teachers, not surprising comprised of many people of teachers in their day jobs. Jim, I assume you're going to open up for questions. But could we perhaps have some folks who worked actively on the final stages could we have an opportunity and I reserve the right to speak after them.

>> Eric Lander: So noted. Others who contributed to the program. Craig Mundie.

>> Craig Mundie: One of the things that I think was notable in the evolution of this report was when we started the discussion, many people said we see the MOOC phenomena happening, but why is it any different? As Rick said, many institutions have been teaching online courses or providing online access for many, many years. And I think the thing that we ultimately concluded, and I would like to emphasize, is that in this case it's about the data. That the level of instrumentation that's possible now, no matter whether the scale is massive or small, the degree of instrumentation of the process of interacting with these systems is unlike anything that the educational world has known in the past. Because of that, we think that there's a potential to think about sort of two different levels of feedback happening within the educational environment. The lowest level is to use the data to personalize the presentation material. So this is more than just a question of giving it out in small doses, but in fact

allowing the system to guide the student through the material in alternative paths that are customized, personalized to each student. We've never really been able to do that as well. But I think perhaps equally important, the data in the large, particularly if we can aggregate it as the recommendations encourage in the third case, the ability to think about evolving the pedagogical system itself at a higher rate of evolution is equally a huge opportunity. To some extent the model of pedagogy that we have arguably goes back at least hundreds of years if not farther and has been very slow in its refinement. And we think this in fact could be one of the major disruptions. And while that may cause some pain to the classicists in the educational system, we think in the end it will facilitate getting the full benefit of the tremendous investment that the country makes in education its citizens. And it's all about the data and how we apply the data both for the benefit of the individual of the student as well as the improvement of the total system. Thanks very much. Shirley.

>> Shirley Jackson: This is reinforcement of what you've heard I think the important point has to do with the fact that there are concerns that people have with the costs of education, the cost of higher education. But there's also a concern about the effectiveness. And so this gives us the opportunity to have a more data-driven approach, having to do with competency development skills development, etcetera, and to even evolve and develop new metrics for measuring the effectiveness of teaching in terms of what one is trying to impart to students and is it a question of skills, is it a question of maturation, which is where typically the residentially-based pieces come into play. And the extra and co-curricular things that universities in particular do. But so I think it allows us to more sharply delineate how students learn and what is important and how best to target to different groups of students. An important focus then is on cognition and learning, populations of students, et cetera. And so but I just want to reinforce what Rick said at the beginning, namely that these are early days yet. And I think as we go along, we're going to learn more. And I think that's embedded in the message to the President.

>> Dan Schrag: Shirley's comments echo pretty much what I was going to say. I think the key is that for whatever reason, this MOOC movement has really been infectious in terms of the enthusiasm for exploring new pedagogical modes across virtually every college and university in the country. That's incredibly exciting, the level of engagement and level of experimentation going on. Now, many of these experiments are not going to be good ones and that's okay.

>> Eric Lander: They may be good experiments they may just fail. It's an important distinction. The experiment --

>> Dan Schrag: Absolutely. Correction.

>> Eric Lander: That's why they're experiments.

>> Dan Schrag: I think the key is that there's an opportunity here that we see, not just to trade teachers for video screens as some people have portrayed this technology. That's really inaccurate. And what Craig was describing was an ability to collect data nearly continuously instead of a big test at the end of the semester actual continuous evaluation and adaptive teaching and learning platforms with peer to peer interactions and all the rest of that that allows for much more sophisticated measures of effective teaching. And that's where we think the technology should go where you both would potentially lower

costs over the long run but more importantly raise the quality of education by actually beginning to measure outcomes and that's very exciting.

>> Eric Lander: Barbara.

>> Barbara Schaal: Another point I wanted to raise was the tremendous potential for this to enhance and expand education, particularly I'm looking at it as a dean from a four-year residential colleges and universities. One of the things I think all of us know no matter what field you are, whether it's art history or physics is that the amount of knowledge is really expanding. Universities and colleges cannot keep up and have faculty that have expertise in all of those areas. And so it's possible by these online courses to really not only offer courses that you can't do within the university or college but also preserve some of that information. For example, in biology, traditionally biology looked at bio diversity, understanding the range of living organisms. It's not what we do so much in biology anymore. Many of our departments are focused on molecular biology or population genetics or genomics, but yet for the good of the nation and for understanding of biology, we really need to preserve that expertise that tacks on specific expertise. This offers us for the first time the opportunity through very careful preparation and with our understanding of enhanced learning, the ability to really offer those courses across a wide range of universities. It's actually very exciting.

>> Cristopher Chyba: My comment follows on Shirley comment. I think many of us view critical thinking as one of the most important objectives often an implicit one in university education. It's hard enough to assess how one is doing in that score in a typical environment. And I won't pretend that we assess that well currently. But, Rick, you mentioned specifically that it's unclear how MOOCs are going to perform in that respect. Could you say a little bit about how we might find that out, when in the future might we be able to compare, or is that something that is, that we're not going to be able to do due to the difficulty of metrics and even the traditional realm.

>>Rick Levin: I think that there's already been some thought given to how one might do this through on these MOOC platforms. Obviously checking for critical thinking and sort of creative intelligence usually requires either oral interaction or written students writing papers, expressing an argument. Staking out a claim. When educating 10,000 people in a class, obviously how to make that happen becomes a more difficult question. Some of the courses that are being offered are experimenting with peer grading and with peer conversation as a way of testing and refining people's arguments. Students criticizing drafts of other students. Them being revised -- having them revised. I think there will be opportunities to sort of see if the technology lends itself to a kind of different kind of interaction between teacher and students and students to student. Here the scale could be -- where the scale's an advantage in terms of collecting data can be an obstacle in terms of good implementation of developing critical thinking skills. But I think a number of the instructors who I know doing courses like this are trying to think about that, are trying to think about are there creative ways to essentially crowd source education in critical thinking instead of doing it all directly by contact between the professor and the student. Susan.

>> Susan Graham: There's another opportunity that I think this technology is going to provide. And that's the opportunity for students to take risks. So that we might be able to use this as a vehicle to

encourage women to go into STEM fields, to encourage people who lack self-confidence to try courses in disciplines that they shy away from. Because of the feedback of the interaction, because of the relative privacy for a student, a student who is worried about appearing ignorant in the privacy of his or her computer interactions can take that chance. It's an opportunity for the field to try to solve some of our societal problems by the ways in which we use this technology.

>> Eric Lander: Mark Gorenberg.

>> Mark Gorenberg: There is another side effect that's valuable for the United States, there are universities overseas particularly in China that where a majority of their curriculum is on Edex, which is the educational platform that Rick talked about that started by MIT and Harvard and now has about 20 universities that have rallied around it. The opportunity for this to be the next generation of what was the Peace Corps or USAID at its finest is a great opportunity for this country to really export its knowledge and really change the world's view of the United States. And that's something that hopefully can build a consortium with the state department, with USAID and other parts of the government and could be a really positive force for good.

>> Eric Lander: That's great. And Chad.

>> Chad Mirkin: I have to say when we first started this, I was probably the most skeptical about what these would be used for. But this whole exercise has convinced me that it's really about five things. The quality, the speed, access, the breadth, which I think Barbara brought up, which is absolutely essential if you think of the amount of material we have to teach and convey to students at the time stays fixed, unless we want to make these very long degrees, yet there are so many different opportunities out there. So many different things that people need to learn and want to learn and this gives you a much better way to personalize that experience as well when integrated with some of the conventional ways of teaching. And of course the cost and the data. And those are the things that I think make this the perfect storm that allow you to really do this right for the first time. When we look back at all the different experiments in terms of online learning and teaching on TV, correspondence courses it didn't have all those components and that makes the difference here.

>> Eric Lander: Shirley, you're back up again, Mark are you planning to be up or --

>> Shirley Jackson: I do want to say, and I think that's something -- I think Rick intimated this -- that is something that one has to keep in the background. At least if you look at residentially-based education they really are parallel universes that exist at universities and the main universe has to do with all the academics and how students learn and so forth. But the parallel universes have to do with what the students do among themselves, and I think there's some interesting things with the MOOC format that relate to how students teach each other. But then there's a whole parallel universe of support and support services for students that have to do with their maturation with learning disabilities, with psychological things, with other social things, that in many ways those who focus the most on the academics don't all the time think about. So I think in the end we're going to have to think about what the crossover and linkages are between these parallel universes in universities. And I say that as the head of the university. And I see the parallel universes every day of the week.

>> Eric Lander: Pat.

>> Pat Falcone: I wanted to ask a question about the second recommendation. About these accrediting bodies. It's my understanding that they're privately run and regional in nature. They don't always agree. They're not necessarily consistent nationally. The rubrics. And there's sort of maybe not as much transparency how those rubrics were making the decisions that apply to the different kinds of programs you talked about, particularly the training, maybe more at the associate degree level, for example, and so I guess I was wondering what exactly encouragement means and what kind of national role there might be.

>> Historically the Department of Education has commented about accreditation and communicated with the accrediting bodies, although they don't control them, that's all I really meant to the extent Department of Education has interaction with accrediting bodies they ought to be pushing in the direction of encouraging their flexibility, their response to innovation, it's literally as simple as that. The prior administration they spent a lot of time beating up on accrediting agencies and at one point there was talk of trying to take them over. So it's not like the Department of Education has to sit completely silent on this matters.

>> Eric Lander: Craig Mundie may be the last comment here.

>> Craig Mundie: Wanted to add a last comment to Pat's question. Another thing that could happen here and the reason we talk about, for example, certifications and other things is that employers are increasingly willing to accept certificates that have nothing to do with classical content of accreditation. And as these systems allow us to basically give people certified training or capability in areas that may either be components of a degree program or even adjunct to it, we may find that the power of accreditation in some sense is diminished because the markets will demand the alternatives. While we can encourage them I think it's important to point out that the market may speak as to what the credential is that the business community is actually interested in seeing. And if they don't adapt to allow these things to happen they may be displaced just by the action of the market.

>> Eric Lander: I'm struck -- I'll make observations hand it back over to Jim here -- I'm struck by the extraordinary breadth of comments and observations about where we stand right now. When we went into this, I think we thought about MOOCs in a sort of unitary way. Now there a whole lot of lenses. It's the data, for example. This iterative ability, what they call in education formative assessments. But at a really rapid scale to learn and adjust instruction. That's one aspect. Or it's the student cohort, interacting with each other, which isn't necessarily the same thing as data. You can have all the students working alone still have data interaction. Maybe it's the students interacting. It's the unlimited course category, what wiki did for Encyclopedias, this would do for the entire educational offerings and make sure you can still take a course in taxonomy even though the university might not have any taxonomists and it's the unlimited shopping period that allows you to take courses. And what skills can you actually learn? We don't know. It's clear you can learn some competencies. How far can you go on critical thinking? We don't know. And how for almost no charge can this be the way that the United States can contribute to the 21st century developments around the world by the sharing of knowledge.

That's not a bad set of possibilities to be thinking about here, but I think what informs all of what the PCAST has talked about is a sense of humility. That it's impossible to know where this is going to go other than it's very interesting and I therefore like the recommendations here about letting market forces play out, encouraging flexibility and in order to really get the value, supporting research and sharing results and making sure to the maximum extent possible data are available so we can all learn together. I think it's great guidance. I'm going to turn back over to Jim for closing remarks here.

>> Jim Gates: Thank you, Eric. I must admit that you channeled me very well just now, because a number of the things you said are on my mind. There's one final point that I'd like to put out in sort of this public forum or semi public forum. And this is a matter of something that we haven't really talked about but I think is extremely important. Most of our focus has been on STEM education. But we all know there's a large domain out there that's outside of STEM education. And recently at UVA there was a very interesting chart that they put out looking at 14 different academic disciplines and 11different occupations. And among those, science was the only one that contributed to all 11occupations among the academic to all 11 occupations. But English and literature and the non-STEM domain had exactly the same attribute. It was the only academic area that contributed to all 11 of the occupational areas. And so the last thing that I sort of -- we didn't talk very much in this report but somehow I'm thinking and hoping will be an outcome here is that the push towards education and technology as it is used within the STEM domain could well trigger a couple of things outside. One of those things is to join in conjunction with a movement called digital humanities, where in fact, if you stop and think about the liberal arts and the classical traditional model for how the liberal arts work, it's essentially a model based on reading great texts. But you can imagine data input from real world almost contemporaneous events being the text from which students learn about how humans work in the real world. This to me is an extremely exciting possibility that our investment in talking about educational technology on this end ties to. And then the other thing is as mentioned by several people around the table, our concern for the rate of increasing costs of higher education in the country is alarming, to say the least. The President has spoken about this in numerous occasions. And so if this technology can bend the cost curve, it may have a very interesting effect in the liberal arts, because we hear stories of a lot of young people that come to universities and colleges who might wish to major in the liberal arts degrees and humanities but feel parental pressure to major in something that people say is directly going to lead to a job. If we can lower the cost of college, maybe we make more spaces for people who have interest in the liberal arts and humanities to pursue those interests. In a very real way borrowing from my colleague Dan Schrag, maybe Ed IT could save the liberal arts and humanities in this environment. I think it's an interesting proposition.

>> Eric Lander: Heavy burden for us to take. I don't know if we can, Rick.

>> Rick Levin: One last point when I listed the members of the working group on this report, I failed to turn my head to the right. So I want to acknowledge Bill Press was also involved.

>> Eric Lander: Absolutely. I think much has been said here about the interests and opportunities. I'd like to call for a vote at this point. Indicating because we owe an enormous tremendous debt to Marjory, Knatokie, and Danielle and I'd like to express that also. [Applause].

>> Eric Lander: One might imagine having a report in which virtually the entire PCAST gets involved expressing opinions writing pieces and all that would just happen by spontaneous generation but it turns out to not happen and we're grateful for the remarkable staff of PCAST to make this possible. I'd like to call for a quick vote. Do I have a motion to approve this report. I do. A second. I have. Those in favor? Any opposed? It's unanimously approved. We will have some editorial work as usual to make sure the report is in good shape for release, which we hope to do very soon. Thank you all. I'll turn back to John for our next subject.

Cybersecurity Report

>> John Holdren: Thank you. And the next topic is the report on cyber security. And to lead that discussion I will call on one of our vice chairs and a leading architect of the cyber security report

>> Bill Press: This is a piece we hoped to bring to you in October but the whole government shut down. This was just one of many, could it be millions of useful government activities that were caught in that maelstrom. But we bring it to you now. As you recall, PCAST has been in the space of cyber security previously in the context of classified report. But there are many aspects of cyber security that we felt are very important to present to a larger community and in no way classified, and that was the genesis of the report that we're going to present to you now. Figure out which button. There we are. This was a small working group of PCAST members. Craig Mundie and myself. From able help from the staff Lauren, who was with OSTP, has now moved on and David Pritchard. I want to give you a couple of slides general introduction before moving quite quickly through our findings and recommendations. If you go back just two or three years, cyber security, cyber defense was supposed to look like a medieval castle. There's the various rings of defense, firewalls and port scanning and I'll let you read that sort of thing. But the real point was that the accepted view of cyber defense was it was all about hard walls and static defenses something that we would now call hardening. Well, what a difference a small number of years makes, because now it's generally recognized, both out in the private sector and within government, that cyber security is about processes that continuously couple threat protection to reaction on all time scales. There has to be a closed feedback loop in it. I see that the E on sense somehow drooped there, but the idea is to sense the threat, react to the threat and sense how well you've done and improve your defense for the future. Now, you might say how often am I supposed to do this? Once a year, once a month, the answer is all the above. And there are different aspects of cyber security depending on the time scale. On the scale of years we're talking about how software and hardware are designed. On the scale of months we're talking about are you keeping your systems patched, are your configurations good, are you using self updating software. We get down to days, also important for patching, operating systems, hours where we're trying to detect signatures of actual malware as is done by most current virus checkers and Internet security packages. But the important frontier which is already with us is in this seconds to minutes where we need user nodes to not only be the best defense they can but to provide information back to the network, back to the nodes to take action and all the way down to milliseconds because that's the scale on which massive attacks could occur, and it's a scale on which one could take responses without a human in the loop, those responses might simply be to disconnect from the network or to reconfigure in response to attacks. That's also the scale in which one has to think about in a cyber conflict between nations or with non state actors what

the national defense response would be. Those two slides I hope motivate what the overarching finding is of this report. The overarching finding is the cyber security will not be achieved by a collection of static precautions that if taken by government and other organizations would make them secure. Rather, cyber security requires a set of processes that continuously couple information about an evolving threat to defensive reactions and responses. And if you understand this overarching finding, then you'll see that our six principal findings under that and the recommendations under that basically flow from this. Well, our first finding is to ask the government to look at itself. Sadly, the federal government today rarely follows accepted best practices. Now, we had a lot of debate on should we say sometimes. Should we say could do better? In the end, we came down very strongly that this is an accurate statement of the situation today. The federal government needs to lead by example. That's my little graphic there. And accelerate its effort to make routine cyber attacks more different by implementing it on its own system. We have a set of recommendations, I won't try to read all of these to you, that are basically common sense things that the federal government should simply give higher priority to. Phasing out insecure operating systems, since modern operating systems are vastly more secure than operating systems whose technology is 15 or 20 years old in some cases trusted platform module is basically to say that we need the hardware to have the hook that allows security related functions to be built on top of them. The most secure browsers facilitate the prevention of identity theft, it's important that we have those. We need to move towards nationwide availability of proofed identities for people, roles, devices, and software. Now these will be completely voluntary in the private sector. The private sector may find it useful or may not find it useful to adopt these in various situations. But the government is different We think there should be mandatory proved identity within the government when there are exchanges among federal data users. That's something that the government can do to lead by example. The federal government should use the best in automatically updating software including cloud hosted software both for commercial off the shelf products and for its own government products. So let me move to finding two. Finding two moves us out into the private sector but only into that limited piece of the private sector that already comes under federal regulation for one reason or another. And we think that in such cases there are real opportunities for promoting and achieving best practices in cyber security through the regulatory agencies that already exist and that already have statutory authorities to go in this direction should they choose to do so. Let me give you the recommendations that follow from that. Now, I want to point out on this one, there aren't many recommendations that begin by saying something should not be done. But this is such a case. The recommendation is that within already regulated industries, the regulator should not require a specific list of cyber security measures. Of course, there's something that we do want them to do and that's the second half of that. We want them to record auditable processes where processes are adopted and the important point continually improved. The second recommendation essentially makes this a little more specific, we think that in the case of independent regulatory agencies, that don't directly come under the executive control, we think the president could strongly encourage regulations that require self reporting and continuous improvement. And we think that a good example in which, on its own, the agency has taken preliminary steps we'd like to encourage more is the SEC. Because the SEC is charged with identifying for the benefit of investors what are the risks in publicly held companies. And we think that the SEC could look at requiring more disclosure of public companies what their cyber risks are more importantly it's the diagram in the left what their plan is to improve their position on those cyber risks on a continuing basis because we think that is material to decisions that investors will want to make as cyber threats increase we want continuous improvement on the left. We don't want the angry man on the checklist on the right. I don't know if he's really angry. He maybe a paid professional angry man. Finding three takes the same spirit further into the private sector. And here the role of government is quite limited are the way to go that these are likely to create an effective cyber security culture, more so than the angry man with the checklist on the previous page there's a history of this direction in the human safety enterprise. Human safety has been vastly improved over the last generation in industry by the understanding it's a continuous improvement it's not a checklist based process. We want to pull that over into the cyber domain as a way for industry to think about this. So the recommendation here is that government's role is to simply encourage this out in the private sector, consensus based standard, and transparent reporting of whether those standards are being met by individual private sector entities. Our fourth finding addresses, I should say is still out in the private sector, where government only has a limited role. But we think it's important that the private sector develop means of sharing among itself on all those time scales that I indicated before, cyber threat data. This would be the kind of thing I'm under attack, so I know how to disconnect or reconfigure some of my networks, but I may have customers or suppliers or other firms in my industry with which it would simply be a good thing to have means of sharing this kind of data. Now, in appropriate circumstances, and with interfaces that are well understood publicly, and therefore accepted by the public, there could be some sharing here between private sector entities and government. That as anybody who reads newspapers recently understands is a very tricky area. So I want to emphasize the main thrust of this finding is simply what the private sector should do itself among firms in the private sector. So what is the federal role, because we advised the federal government. The federal role should be to facilitate the establishment of private sector partnerships that make this possible, that make possible the exchange of threat data among potentially vulnerable private sector entities. And the immediate important point is that for this to be effective, these data flows should not be and would not be accessible to the government, although the government might participate in establishing protocols in setting up the means for the private sector. Our fifth finding addresses Internet service providers, ISPs. You're not supposed to read the fine print in the little picture at the bottom, except to notice that the users are clustered around the cloud and between the users and the cloud live the ISPs, the Internet service providers, or their equivalent organizations within large corporations who perform the same functions and because the ISPs are above the level of individual users but are not yet as we might think of them inside the cloud where everything's become hard to find, we think that they can play a unique role. Again, the federal role is quite limited here. We think the federal government should establish policies that describe what is desired behavior by ISPs what are best practices or perhaps what are minimum acceptable practices for ISPs. And then we think that NIST is a great organization, in the executive order on cyber security for a number of purposes one they're moving out smartly and we're happy to see what's happening out there is talking to the ISPs and establishing standards for voluntary measures by which ISPs could alert users and direct them to appropriate resources if their machines or devices are known to be compromised. Our 6th finding addresses future. And that's research. Future architectures are going to have to start with the premise that they live in a hostile environment. It's not just that your computer is an enclave and that the outside of it is a hostile environment. Your computer inside your computer, there are enclaves at various levels of security and with varying levels of risk of bad behavior. We need research to understand how to build secure systems in these dynamic environments that do not always share assumptions of what are trusted components. So our recommendations are when has PCAST ever made a report that didn't call for more research. There's a reason for that. And in this case particularly we need more research in universities and industry on how to build high assurance computer systems. We think that there would be a useful role for an independent organization tasked with development of certifiable maturity levels with respect to the kinds of design processes that would come out of this research. And finally we think that there's a need for high risk, high return basic research in this area. The kind of thing that would have only, that might pay off on a 10 or 20 year time horizon but when it does pay off can fundamentally transform the way we think about cyber security today. Yes with that the working group commends this report to you I wish I could have done it a month and a half ago and we hope you'll consider it for adoption.

>> John Holdren: Thank you Bill. Let me ask Craig Mundie as the other member of the working group if he would like to add any thoughts.

>> Craig Mundie: No, I think Bill did a superb job summarizing the report and recommendations and I to do endorse it and hope people will approve it.

>> John Holdren: Let's open it up to other PCAST members. Starting with Ed.

>> Ed Penhoet: Several times in your report you call for auditing to be performed, who will perform these audits you talk about in the record.

>> Bill Press: Good question we're not thinking about these being audits from government agencies. Again our model is the human security and safety model where once industry adopts this model of continuous self improvement, a whole little eco structure gets created. In the case of human safety, there are outside firms that come in, third party firms. For example, Dupont, which had made a reputation over decades as a very safety conscious company, has spun off several separate entities that do human safety consulting and auditing for industry. So our view is if we get the incentives right, we can get that same kind of private sector ecosystem going for cyber security.

>> Very well done Bill and Craig you talked about cyber structure and all and you mentioned the SEC one who has done good   do you see the government exchanging best practices like the SEC with some other financial groups within the government or even non financial?

>> Bill Press: Certainly. And certainly that's the thrust of what NIST has started to do in response to the president's executive order. I think the key transformation, this is probably about the tenth time I've said this, is to get away from thinking about checklists and to get to thinking about continuous improvement processes and certainly we wish that on the government every bit as much as we wish that on the private sector.

>> Craig Mundie: I'd like to add to that. Our belief is that companies the government both find themselves in a situation where they have to advertise sort of organization by organization, where they are relative to let's say this year's best practice, it turns out there becomes a lot of public pressure for

them to essentially keep trying to get up to the level. And so we're a lot more interested, sort of speaks to the auditing question, too, of not having the sense of private accountability or auditability to a checklist but rather public accountability to the best practice that's established sector by sector. And what we recognize is things are so complex here, that what works for the banking industry and may be considered sufficient may be completely different than what would be required in the power industry, who has a much greater SCADA exposure, for example. That's why we don't like the checklist model, is one we don't think it moves fast enough and two there's no unifying theory of checklists that would make you secure. And so we're a lot more interested in publishing who is the best this year and then getting everybody else to be able to self declare how they stand relative to that.

>> John Holdren: Michael McQuade.

>> Michael McQuade: Very good set of recommendations on the piling department I'd sort of maybe just draw the connection between sort of the assurance and auditing and sort of more holistic non checklist version of things, but there also is, this is not just sort of assurance of computational capability or system capability being available. There are significant safety issues, whether they're mission critical safety of delivering power or mission critical safety for transportation systems, et cetera. So I think the connection to how safety has been looked at as a process as opposed to a set of checklists is exactly the right approach here.

>> John Holdren: Good. Chris Chyba.

>> Christopher Chyba: This is a very speculative question for Bill and Craig. Suppose you could go back to the beginning of time to the start of the Internet and the Web and redesign it from the bottom up on the assumption that you were in a hostile environment rather than the way things progressed would it be possible if you had started that way to have each computer be an impenetrable fortress, that is to say, is the conclusion that we have to have this kind of dynamic defense historically contingent conclusion, because of the way things in fact evolved or was it inevitable? Did it have to be the case?

>> Bill Press: I'll give you my three what I would have done differently. I wouldn't have programming languages be what they are today because they don't allow us to use the computer to determine the correctness of the computer. And that's just an unfortunate byproduct that programming languages have evolved. If I could go way back I'd get the whole industry to have started down the path to a different model of writing programs. The second is, that you need identity. Strong identity. That's a key component of this because without identity there's no deterrence. Because you can't attribute problems. Just like you have in nukes and bio and other things, if you didn't know who the bad guy was, then he operates with impunity. And that's unfortunately the problem we have today is because we didn't build robust identity into any of the key things, that's why here I think for the first time you see in a public recommendation, that it's not sufficient to just know the people. You have to know the people reliably, the computer itself reliably, the Providence of the software reliably and the role that people are participating in. And unless you can do each of those things in a reliable way, you start to fail. And the final answer to your question is one of the real threats, and the reason I think that this moved to a more process oriented it would have been inevitable in any case is because you're now building complex

adaptive systems that come from interconnecting computers, each of which might have thought to have been perfect relative to its own spec. But you get emergent behaviors in the interaction between them. You see this even in the flash, crash, the stock market, why do they have circuit breakers to stop trading. It's because in fact they have not been able, even in the narrow confines of just a trading system, for example, to at scale understand the behavior of the system in the large. And so because of that, I think that we would have found that even if every computer had been perfect in every regard, one at a time, at the moment it was developed, once you cross connected these things, you get the emergent behaviors that are completely unpredictable. In fact, one of the detailed components of our research recommendation points out that unless we can start to actually get a handle on emergent behavior, and figure out how you want to control it, that that too will become a long term vulnerability. It's also why we think it's a hard problem in this 10 to 20 year research program.

>> Bill Press: I think that's a great question in fact I heard Dave Clark from MIT give a talk on this recently one of the real Internet pioneers, of course people are always saying you guys got it wrong you should have done it differently. And his response was in the most part, if he could do it over again he would do it pretty much in the same way because they understood there were security threats but they thought they were just providing a pipeline and the pipeline should be completely transparent, allow threats, allow everything, and that the security would be done at the ends of the pipeline. But he admitted the one thing they didn't foresee is denial of service attacks. Because that then fills and chokes the pipeline. And it's there where this model of it's somebody else's problem just can't work and it's got to be your problem, the Internet backbone provider's problem as well.

>> John Holdren: Well, seeing no more flags, Bill, do you have any closing comments following these interventions?

>> Bill Press: No I think I've said everything too many times already.

>> John Holdren: That being so, let us   [off microphone] . I move.

>> John Holdren: Second. All those in favor of approving the report. [Off microphone] we are astonishingly a little bit ahead of schedule. But I'm going to call the coffee break, which in our original schedule I think was supposed to be at 11. So let us have a 15minute coffee break and return just after 11:00.

Privacy Discussion

>> John Holdren: The Deputy Chief Technology Officer CTO sitting in OSTP with responsibilities for privacy. And as well as Internet policy and innovation. Prior to joining the Obama Administration in July, Nicole was the legal director for products at Twitter and from 2004 to 2011 she served as Google's vice president and deputy general counsel primarily responsible for the company's product and regulatory matters. She also was the co editor of a volume called electronic media and privacy law handbook. Her

law degree is from the University of California At Berkeley. There is more, but I won't take more of her time by reading you more of her bio. Nicole, thank you very much for being with us.

>> Nicole Wong: Thank you Dr. Holdren and Dr. Lander. Pleasure to be here to have the opportunity to address the council. I also want to thank Rick wise and Marjory in helping me prepare me for this session. I'm pleased to report that I'm on my fifth anniversary as a member of the White House. As some of you now I hail from the Bay Area where I worked for Google for eight years and then for Twitter and where I understand it is currently 20 degrees warmer than it is here. And I'm adjusting to both the weather and the acronyms that come with government life. So today I'm going to go old school on you. I'm not going to have a PowerPoint. But I just wanted to talk a little bit about the topic of privacy, which is occupying both headlines and policy circles and technology circles. In my previous jobs, I had primary responsibility for the launch of the products of those companies. And that meant having compliance in the various legal regimes around the world, whether it was copyright or trademark or consumer protection laws or content regulations. But the most difficult and increasingly complex area was always privacy. So in my new role as deputy CTO, I again focus primarily on Internet and innovation policy and in this age of information, privacy is also a critical component of the work. You're all well aware that the volume and velocity of data is greater than ever. Indeed, as PCAST's recommendations, for federal networking and IT R&D reflect, we need cutting edge research to help us distill the value from the growing availability of data while protecting the privacy and security of personal information. In the more than 18 years that I worked on privacy issues, I do not recall a time when our government faced more scrutiny about its policies and practices in the use of data. We have been fortunate to witness the exponential growth of digital technologies that empower citizens, fuel economic growth and provide the foundation for further innovation. Given the quickly changing nature of technological capabilities I think we all recognize that it is time to take a close look at how and for what purposes various entities, whether they're public or private, gather and use information. So last year, recognizing the importance of affirming the privacy values in the context of these new technologies the president announced the first ever consumer privacy bill of rights as a blueprint for the privacy information age setting out principles and expectations in the commercial setting. And, of course, the recent unauthorized disclosures of U.S. intelligence programs have drawn particular public attention to issues of privacy and national security. We are at a difficult and formative moment as a nation and as global citizens to reach some kind of consensus about how best to apply our privacy values in light of national security challenges. It is again in this context of this dynamic technology environment that the president has directed a detailed review of the nation's surveillance capabilities. This review is being led by the White House, and it includes agencies from across the government. There are also important efforts underway that will enable others to review how the government is doing in its efforts to achieve both privacy and security. Including the review group on intelligence and communications technology and the privacy and civil liberties oversight board. Because these reviews are still underway, I'm not going to directly address privacy and national intelligence programs during this session. But I do think it's important for us to note that the government is not alone in seeking to find the right balance between the powerful benefits of data to individuals, organizations and society and data's potential impacts on privacy. This is a conversation happening in industry, in civil society, in academia, and so today I'd like to talk about privacy and the privacy environment more generally and to do so through the frame of your

recommendations on privacy research from earlier this year. Well, studies show that most folks will say that they care about privacy. As a society, we still have a lot to learn about the nature, meaning and appropriate protection of privacy and the means of the technological psycho sociological realms it's difficult to get privacy policy right without a basic understanding in these areas which is why I so appreciated PCAST's recommendations in case you need a reminder what that recommendation was from January you wrote: NIST should create a multi agency collaborative effort led by NSF, the Department of Health and Human Services and DARPA to develop the scientific and engineering foundations of privacy R&D.NIDRR should coordinate across government agencies to develop deployable technologies and inform policy decisions. Shortly after I arrived in August of this year OSTP requested information about the state of privacy R&D across NIDRR agencies to get us started. NIDRR is continuing to compile the information and importantly this request for information is not a substantive assessment of the research so we're not yet in a position to provide specific recommendations about the direction of federal research. But when the process concludes and with the more comprehensive view of the various privacy research areas, we plan to assess the current activities to identify opportunities for multi agency coordination and to explore possible agenda on the foundations of privacy research and development. That said, I have gotten a preliminary overview of some of NIDRR's findings and I do have some interesting observations at this stage. First, we actually asked the agencies to provide a definition of privacy research. And found that there are significantly varying definitions on what constitutes privacy research from activities that support privacy principles like control and transparency and security, to very specific research and statistical confidentiality, identity verification and data security. Some agencies did not report any definition of research NIDRR reported many agencies don't report any definition of privacy review research or guidance I'll come back to that in just a minute. As a second observation, NIDRR roughly grouped the research into four areas, research as a privacy extension of security such as improving security on mobile platforms, research characterizing privacy objectives and establishing compliance regimes. So that appears to be not scientific research per se but integrating privacy requirements like notice and security into existing standards and frameworks. There was a research assuring privacy in healthcare in the context of healthcare privacy laws and research exploring basic privacy constructs in their application in information technology. Which basically covers a host of wide ranging NSF research that examines the formulation of privacy expectations. Within these four areas, there do appear to be specific research projects that address some of the issues PCAST outlined in their recommendation in 2013, such as how to achieve cyber security and security more broadly without unnecessarily disclosing individual information. And it's worth noting that in addition to the ongoing agency research, the administration launched a separate public/private big data initiative which includes NSF working with MIT to explore some of the unique issues around privacy in the collection and use of large and diverse data sets. On the other hand, the current set of research does not reflect coordination across the agencies or even a common prioritization. And that's not because NIDRR's not capable of doing such multiagency coordination, they do it very well in the area of, for example, cyber security. Rather, as a mentioned before, we as a society have yet to agree on the contours of personal privacy. So it's not at all surprising that the agencies don't quite agree on what constitutes privacy research. The definitions of privacy are still evolving. Coming up with useful definitions for privacy itself is an active research question. So in the remaining time that I have, I want to focus on this issue, the problem of defining the privacy problem. And setting a rational course for addressing it in our research and in our public policy. We are at an important moment, an inflection point of the scope and scale of data and its potential uses, and in which social norms about privacy are still in flux. There's general agreement that privacy has a value but not agreement on its parameters or its weight. So for some people privacy concerns arise from identity theft and for others it's about intrusive advertising or government surveillance or human dignity. Privacy is fundamentally defined by our context and our culture. And developing the norms about the proper use or protection of data takes time and the efforts of a constellation of players that includes technologists and industry and government and civil society. That's a broad constellation. There's no obvious hierarchy to the process of working things out. So Paul Om, a friend and professor at the University of Colorado . He's recovering computer crimes lawyer with the DOJ and consultant to the FTC repeatedly reminds me in the area of privacy lawyers think the answer lies with technology and technologist thinks the solution is up to the lawyers. I think it's both and more. How should we think about the squishy values of privacy and their relationship to technology? Two years ago I taught a graduate class with Dierdre Mulligan we crossed the class with two schools got a mix of students law and public policy students the title which I don't remember because in the academic tradition had too many words and it was something like Internet policy and challenges on global platforms, part of our conversation was about how do we embed values, like openness or transparency into technology. The Internet, of course, was built for openness and transparency and continue annuity and importantly if you ask Vint Cerf flexibility because the creators didn't know what it would do those are values embedded in the technology and they've served to frame the development of not just the architecture but also indirectly the innovations and the policies that have grown out of and apply to the Internet. You may know that there's also very active discussion among legal practitioners and scholars and regulators and policymakers and most importantly technologists about embedding privacy in technology. In those circles they call it privacy by design. And for the most part these have been distinct circles, the lawyers, the policymakers, the engineers, but in the last few years, take, for example, the do not track protocol discussed at the WC three those circles have been converging, the success of the W three C and do not track is still to be determined but the collaboration between these three communities is unavoidably and correctly the direction we must follow for sound technology policy making. I've spent the bulk of my career as a lawyer for Internet companies, working with engineers, some of whom, yes, very much discontained lawyers, suits and rules in general. They like to build things. Particularly things that are audacious and cool and they like data a lot and a lot of it. I've also watched governments scramble to keep up with the dynamism of this technology sometimes with excellent outcomes and sometimes not in the area the advance of our capabilities makes the establishment of norms whether formal or informal challenging which is not to say we don't have norms or rules which is in the United States first articulated the fair privacy information principles in society principles of notice, access, control and security, that continue to be the framework for most of the privacy laws around the world. And as I mentioned earlier February last year the organization announced the consumer privacy bill of rights which is intended to give consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data. In other words, the consumer privacy bill of rights articulates a set of privacy values in the commercial arena based on our commercial commitment to our privacy and affirmation of it as we embrace a host of new technologies. Technologists know what set of values and principles to work against in the design of their products and policymakers we can use them to set the privacy research and ensure an appropriate art of policy making. So bear with me for a few moments because I'm going to get at this challenge by talking to you about seatbelts. And then I promise I'm going to bring it back around to privacy. In my class, I had the students read an old sociology article by Bruno Lature called where are the missing masses the sociology of a few mundane artifacts a seminal article in sociology and technology and he beautifully draws out the notion that technology and human behavior are intertwined in a relationship between the producers, the machines and the users. He starts his article by describing his frustration with his seatbelt early this morning I was in a bad mood decided to break a law and start my car without buckling the seatbelt he goes on to describe how his red card flashes a red light admonishing him to fasten the seatbelt it starts to beep you can almost hear him swearing at the car as they force him to worsen his mood getting him to do something to do he doesn't want to do is break the law the seatbelts and mechanisms make him feel that technology has removed his moral choice about obeying the law and keeping himself and others safe. This notion of a technology, in this case the seatbelt and penumbra of noisy reminders it can encourage or coerce moral behavior is something that can become very deeply engrained and that came to me last year when I went to a movie with my then 11 year old daughter and we sat down in those big stadium seats she reached to put on a seatbelt. She said mommy it feels unnatural not to have a seatbelt. So there's this long history of technology and public policy and law and court cases and public education that move us from la tour's resistance to that coercive technology to my daughter's natural habit. And the history of how we got there can be instructive to those who work in the field of privacy, because safeguarding our personal information is also a story about technology and industry development and resistance and government invention and legal battles and social norm making. And I think we are just at the start of that story. So let me tell you a little bit about the seatbelt. First came the technologists. In 1885,Edward Claghorn nabbed the first U.S. patent for something like a seatbelt although he describes it in the patent applications as having nothing to do with automobiles. And then more than 70 years go by until 1956 when Volvo Ford and Chrysler each include and actively market seat belts as accessory or options in new models. In 1958 Volvo designer bowlan designed the seatbelt that you find in most cars told front seatbelts did not become required in cars in Europe until 1965, and then in the U.S. in the following year. That's 81 years after the Claghorn patent. I'm going to take a minute to describe the seatbelt because it's pretty smart technology. It was designed to be as unobtrusive as possible and simple to operate. So you can easily put it on and occupants would wear it and take it off in an emergency and la tour mentioned it's contradicting two programs to be both lenient and firm in response to humans and the context. This is all well and good but how do you get someone like ascoff law like la tour to wear them because that's the question that many of my former engineers would ask themselves or me as their legal counsel or regulators, it's all well and good for you to ask me to design this beautiful privacy tool, but no one's going to use it. It's too hard to design a product that is simple and effortless and will actually protect your privacy. You cannot make users care about privacy in the midst of trying to get something done. So the story of the seatbelt is more than the story of technology. Going back to my daughter's natural habit. It's also the story of social norm making. And in the history of that seatbelt, it was in the 1960s, which was a time of great economic expansion and consumer empowerment, so car ownership was booming after World War II. And both the automobile industry and technology for the production of automobile parts experienced unprecedented growth. So faced with growing numbers active vehicle owners and consequently road accidents the public was growing increasingly concerned over the rising number of traffic fatalities on the nation's roads. Such fatalities had increased by nearly 30 percent between 1960 and 1965 with over 50,000 traffic related accidents in 1965 alone. And experts forecasted 100,000 such deaths annually by 1975, unless something was done to improve traffic safety. It became the leading cause of death for people under the age of 44 in the United States. So here comes the consumer advocate. In 1965 Ralph Nader published unsafe at any speed criticizing the automobile industry for negating safety in favor of power and styling when designing new vehicles. He went on to testify before Congress in 1966 the government steps in. Congress passed the highway safety act and national traffic and motor vehicle safety act which among other things required the installation of seatbelts. And then after nearly 20 years of regulatory wrangling the national highway traffic administration required states to put mandatory seatbelt laws in place as a result in New York where the first mandatory seatbelt law came into effect in 1985, seatbelt use rates increased from 16 percent before the law to 57 percent 4 months after the law. Fatalities decreased 19 percent, despite the modest increase in mileage driven by September 19, 8934, states had established seatbelt lawsuits, today every state has some form of mandatory seatbelt use except New Hampshire. If you were trying to remember, I believe the state motto is live free or die. This is also certainly more history about the seatbelt than you expected or ever wanted to know. So why? What can we learn? As an initial matter, let me say that there are important distinctions between the story of the seatbelt and our current position with respect to privacy. First, as a society, we still haven't agreed what we want to protect. This is evident in the current and diverse set of research projects in the federal agencies. While the consumer privacy bill of rights sets out certain values for our commercial sphere our public policy debates still reflect a great deal of disagreements, whether it's over national security or the use of geo location information or the use of drones. We still don't have a universal understanding of privacy or agreement on in which context it needs to be protected. This is a serious impediment to rational engineering or policy making. Second we still lack important data. We don't have a FARS for privacy so in vehicle safety they have a fatality analysis reporting system or FARS which contains data about fatal traffic accidents within the 50 states and U.S. territories. That data is collected by trained state employees who translate, transmit standardized coded data about accidents on their respective highways and working off the first problems, we don't have agreement on what we're protecting. We don't have a standardized way of describing it or gathering it or knowing if or when we've succeeded in solving the privacy problem. Third, we don't have a single platform technology. A car is a largely uniform platform distinguished mostly by its features but not by its core function. So on top of that platform you can get a manufacturer's agreement on a universal seatbelt. A technology that's intuitively understood by any user even when that user switches cars fixed by a mechanic and deployable in any country. In contrast one of the hardest things about privacy or data protection is that the data in question are collected on a huge number of platforms. Online and off line desktop and mobile in an array of formats and forms and interfaces. Right now at least no innovator wants to be locked into a universal privacy seatbelt. The good news is that we are seeing a lot of competition to build one. Notwithstanding these hurdles in the privacy arena, there are some key useful insights from the seatbelt story. First, technology design is not the only tool in the toolbox. For vehicle safety, the ultimate goal is to create overall safety, which can be achieved through a range of changes to the ecosystem, including road improvements, better lighting, speed laws, drunk driving laws and public education campaigns. The same is true for privacy. So while it is incredibly important to do the foundational research in privacy that PCAST recommended, at the same time we should not rely on the discovery of a single silver technology bullet. Instead, we should continue to work toward an overall strategy to improve privacy in the data ecosystem. Second, the change we're looking for must be driven for many sectors. We might avoid the decades of stalemate in vehicle safety improvements, if public and private cooperation is cultivated. It's generally felt to me like industry, consumer advocates and regulators who focused on consumer privacy were willing to do this engaged in the challenges of privacy engineering and regulation. But we do tend to stalemate over differences in frameworks, priorities and information. Which is particularly amplified in conversations about global platforms or competing interests insecurity, criminal activity and censorship. As we look at building a research agenda, it's essential that we keep in mind the need for that interdisciplinary model and how to incentivize it. Finally, let me return to the real point of la tour's argument, which is that there's an exchange between humans and machines, where the machine is doing more than assuming a delegated duty likes trapping you in your car encrypting your data. The machine is making you feel more secure. And here we're talking about something that's more than just mere mechanics. It's a situation where the function of the machine can change the behavior of the human. And this is where the science of privacy reveals itself to be more than hardcore cryptography or multi party computation or anonymization methods although all of those play important roles. But we should be mindful that the technology can be used to help shape individuals' expectations and behaviors. Technologies and interfaces that present themselves to a user as a vault create different behaviors than technologies that present themselves as a town square or an open for view desktop. Going back to my first observation that we still aren't quite sure how to define privacy research, I would suggest that we adopt a broad view and a big tent. The signs of privacy is not only about how to keep personal data secure and private, but also how to enable individuals to live in the open, with the flexibility of personas that we enjoy in the physical world. As we seek to identify, prioritize and coordinate privacy research across the government we should ensure we look beyond the network of IT experts. We'll need social scientists human computer interaction experts, civil society. We might even need the lawyers. This work will be challenging, but essential to the continued and healthy development of our digital world, and I very much look forward to joining you in advancing it. Thank you so much for your time this morning. I think I'm able to take a few questions.

>> John Holdren: Thank you, Nicole. First flag up is Craig Mundie.

>> Craig Mundie: I have many comments.[Laughter].

>> John Holdren: And we have time for them.

>> Craig Mundie: We do or do not?

>> John Holdren: Do.

>> Craig Mundie: I think one of the fundamental problems that we have in this discussion is the conflation of the security question and the privacy question. You can have a privacy problem by dint of a security failure, but that's completely different than the idea that as a matter of policy someone intends to make a use of your data for a purpose that you may not like. And I think one of the real challenges in whether you're defining a research agenda or a product, is the fact that when you blend

these things together, it becomes very, very difficult to have a consistent conversation. So the first thing I suggest is that you religiously tease apart the issues that come from breaches on the security side. There we need lawyers. We have a lot of legal challenges. We need to know how to prosecute those things. We have security challenges, which we just talked about in the last recommendation, and I think that the more challenging part, frankly, in this conversation, is the question about privacy per se. And that in that regard we need to focus on that because there the question is what is the intent of the person acquiring the data, the person providing the data, and what are the full spectrum of concerns that could emerge. Second, and this again has a analogy in the last report we discussed on security, is that I don't just as then we said, we recommend against the idea that there can be a checklist, a standard, a specification against which people will perform in the security domain, similarly I would advocate that we shouldn't try to define a standard for privacy. We can't define it. In fact, I contend that in the current environment of the Internet, when people realize there's a new privacy problem, it only comes because there's a new application. And in fact it isn't that people knew they worried about a particular class of use, because it was a completely unanticipated situation. It was only these creative people and the availability of new capabilities in computation, storage and collection of information that produces the opportunity to do something that never was done before, Twitter being a perfect example. And even in cases, I'll use Twitter as an example, where by definition the tweets are all public. People are discovering the collection, the lifetime collection of tweets, all of which were public one at a time, allows a profile of them that makes them completely uncomfortable when taken together. And no one can argue that everything they agreed that they said was public but they never contemplated that the aggregate allowed people broadly to analyze that in a way that they never anticipated. I think it's far more important that we focus on this question of uses as they emerge and the combination of policy, law and technology that will allow us to move away from the idea of dealing with this question as one of control and collection retention to instead move toward controlling usage as it emerges. One things that's different from this as the classical FIPS model or OCED models is in that environment that the people tended to have a discrete concept of I was exchanging data for some benefit, whether it was I give you data you give me a credit card, now the data is collected from so many sources that there's no longer a discrete relationship in the mind of the user between what data I provided, what benefit I may have gotten from it and what the potential collective use of data is in triangulation on me. And as a result many of us in the tech business have decided we have to move away from the idea of retention and collection as a control and two an aggressive model of controlling uses. Happily, there is no use without a program. That is a key concept. And as a result we can start to think about controlling the programs because each of them is a codification of a use that is extremely well defined. We never had such a definition before when the uses were done less programmatically. You did mention that people focus around anonymization and other ideas but we also know that anonymization is largely a myth so I think it's sort of dangerous to perpetuate that as a result we seek to establish a research agenda, I think it's going to be a lot more important to think about what the combination of technologies are that would allow us to control uses. In talking about that I do have things I do endorse we need a multidisciplinary approach but largely in order to determine the best way in which the individual, the institution and the society at large get to make decisions both about permitting and denying specific uses, and there is sort of as you point out a broad array of sort of psychological and policy and legal challenges around that. Finally, I would argue that on the legal side, there is a baseline requirement that would facilitate all these things, that is not adequately developed today, and I would encourage the government to prosecute or to look for. And that is that we do not have law that has sufficient penalties attached to it for intentionally violating the specifications around uses of data. And as a result it's like parking tickets. I mean, if you're driving around you can't find a parking place, you'll make a moral decision to basically say well I'm going to park here and if I get a ticket that's a reasonable cost of doing business and the problem right now there's so many uses of big data where the fines for doing the wrong thing are largely parking ticket class, that there's no correspondence between the economic benefit of sort of pushing the envelope and the cost having a decision made that maybe you pushed too far. And lastly, the whole idea that the government could ever get into the mode of having regulation for every use, I think, is probably not possible at this point. And as a result we need to move more in a direction of establishing a mechanism which has a legal basis that allows all the companies to build to a common facility and have all the individuals and institutions and others assume that that facility exists and will be honored and that a failure to honor it would have sufficient penalties attached. And what I'd like to see is across agency activity that seeks to define that common mechanism. A lot of work has been done by a number of companies. A lot of this has been done with many of the world's data regulators already. Many are recognizing the impending failure of the current regimes, and I want to make sure as you and your colleagues pursue this in the government that you're looking at this broadly in understanding what's going on outside the United States and to the extent that many of the companies have already realized the pending failure of the current model, that we don't let the NIDRR coordination basically continue to invest in the pursuit of research for a model which those who have already faced the big data problem know can no longer succeed. And I think it's essential that we get a handle on that and try to target the investment that the government makes toward novel methods as opposed to marginal improvements to the methods that we had for many years.

>> Nicole Wong: Couple quick reactions.

>> John Holdren: Please go ahead and respond.

>> Nicole Wong: I'm just do a couple of them I'll make sure that other folks in the room have a chance to comment, too. I think you're absolutely right about the very fuzzy line between cyber security and privacy research. And that actually came out I think in the responses we got back from agencies is they didn't know if or if it were proper to try and pull them apart. I caught just the tail end of the last session on cyber security. So I agree that cyber security is a different thing than privacy, although privacy relies on some notion of security of my data, or at least that's how socially people are still thinking about it. I also think if the direction of greater cyber security, maybe the direction of what the next version of the Web looks like, has to do with greater authentication of individuals of computers, of individuals and of the indices of a person, and there was just a recent workshop on the Internet of things here in DC as well. So I can imagine you want that. Like, you want to know when the Internet of things happens we are delivering healthcare to the right person and it has to be the right person, but in that world of authentication, not only is the cyber security critical but so is the impacts on privacy because I know it's you. It's not an IP address that's dynamic and will change in the next few hours. It's not the type of sued anity that people during Egypt during the Arab Spring relied on and others. So I think there's a real

debate over what is the trade off we make when we move from a much more authenticated unsecure Web from what is kind of a still very open and porous Web.

>> John Holdren: The question I wanted to ask is related in a way to some of what you were just saying. But I've been struck a couple times by Craig's comment and the comments of others that anonymization is now pretty much a myth. And the question I have is at what scale of resources to invalidate anonymization is that true. In other words, when you say anonymization is pretty much still a myth, does that mean that any government can create attempts of anonymization does it mean any firm can do it, does it mean any hacker can do it? What scale are we talking about on which that statement is valid?

>> Certainly any reasonable company who has access to just broadly available public databases can do it today. I've been involved with a group of people who are, I think, pretty convinced now that with only publicly available Web based databases, you could give me completely blind a gene sequence and nothing else and I could tell you who the person is. And so I just think that the computational capabilities. In a sense there's no longer a limit even to the individual to the computational facilities, because if you have your Visa card you can call up Microsoft or Amazon and rent the world's largest computing facility for a few minutes. And it comes prebuilt with all the world's largest public databases and it's the intersections of those data sets and whatever unique data you have that allows this level of triangulation. And so I think you kind of have to start with the assumption that there isn't a way to prevent that kind of thing from happening. That's why I'm so personally convinced that what you have to outlaw are uses. Congress did this once with the GENI law already where they recognize we're worried about genetic discrimination for insurance and employment. So we already preemptively wrote that one law. But the Internet just demonstrates you can't possibly expect the Congress to figure out how it's going to write a law for every application of every classification of data. So I think we just have to let it go that this idea that you can hide the data, anonymize the data, what you have to do to this question of identities, you have to say Eric, I like Eric, he's doing research on rheumatoid arthritis so I'm going to give him my genome and it comes with these digital rights that say Eric Lander gets the research rheumatoid arthritis. That's all he gets to do with the data. And then if he violates that, this is my comment about the law, it should be like a felony for intentional violation of that. Because otherwise you just don't have the penalties to deter bad actors, in a world where the data ultimately has to be unmasked for use. And I think we have to go in this direction, and unfortunately most people are still dancing around the edges or talking about refinement about the classical models. That's why I'm encouraging Nicole to kind of really try to focus on these other areas, because frankly the government is not in a leadership position right now in terms of thinking about these issues. And so I just want to make sure that the guidance that we can give through PCAST and OSTP and the NIDRR activities are to try to get the government to leave behind what I contend are the rapidly failing models and focus their own investments in areas that would facilitate and accelerate a move into these other directions.

>> John Holdren: Thank you. We are out of time but Nicole, if you have any closing comments, they would be welcome.

>> Nicole Wong: No. It's a pleasure to be here and meet all of you.

>> John Holdren: Thank you very much for being with us.

Public Comment

>> John Holdren: We now come to the part of our session devoted to public comment. And Bill Press will preside in this segment. Bill.

>> Bill Press: Thanks, John. It's actually today an easy thing to preside over because we have only one person who has registered to make an oral public comment. I'd like to point out that there are other ways that the public interacts with PCAST. We've all received a collection of written comments that were received before our last meeting that was distributed before this meeting. That said, to the folks on the Web out there, come to one of our meetings here and register and give public comment, because we like to hear what you're thinking. With that, let me introduce Jon Pyatt, Vice President Of Science Coalition. Mr. Pyatt, you have two minutes.

>> Jon Pyatt: Thank you. Good morning. My name is Jon Pyatt.

>> Bill Press: This isn't out of your time.

>> Jon Pyatt: I'm director of relations for University of Illinois I'm here in my role as vice president of science coalition. As you may know the science coalition is a nonprofit nonpartisan organization of more than 50 of the nation's leading public and private research universities. And our mission is to support strong and sustained federal funding of basic scientific research. We believe this federal investment in research is essential to the ability of the United States to educate, innovate and compete in a global economy. The science coalition works to find different ways to illustrate the value of this investment. And one such example is a report recently released by the science coalition called sparking economic growth 2.0. It identifies 100 companies that trace their roots to federally funded university research. It highlights the roles these companies play in bringing transformational innovations to market, creating new jobs, and contributing to economic growth, the companies in this report are primarily small businesses but collectively they've already created more than 7,200 jobs boosting our local state and national economies. This report illustrates just one example of what is gained with the federal government investing in scientific research. But it also illustrates what will be lost if the current downward trend in research funding continues and if sequestration remains in place. Were it not for the federal investment in scientific research that occurred years even decades ago these companies, their products, services, jobs and economic growth would likely not exist today. I appreciate the opportunity to highlight this report for you. PCAST cited the 2010 version of this report in some of its materials. And I hope that you find this latest versions parking economic growth 2.0 as valuable to your work. I have hard copies for each of you and to report along with the searchable database of our companies is available at the science coalition's website atsciencecoalition.org/success stories.

>> Bill Press: Thank you very much. With that John back to you.

>> John Holdren: That concludes our agenda for this meeting of PCAST. Again, it only remains to thank the members of PCAST, the OSTP staff, and the members of the wider community who have joined us either in person or on the Web for your participation and your interest. We are adjourned.