



Presidential Commission  
*for the Study of Bioethical Issues*

## **TRANSCRIPT**

### **Roundtable Discussion**

Meeting 10, Session 4  
August 1, 2012  
Washington, DC

DR. WAGNER: But don't go anywhere. No, please don't go anywhere. In fact, what we want to do is invite back now all of our other morning's guests and speakers, if they would join us. And I think we've got name tags up here to remind you who you are.

DR. GUTMANN: While you're getting up there I just want to expand on the contradictory – on the computer. There is a role. Given all the technology and people think of it as doing all kinds of technological savvy things. There is a way of if people check two contradictory boxes that pop up saying you have checked a box that is incompatible with this. Please determine which you believe and sending them back to the box. That's an educational use of technology.

DR. KNOPPERS: And we do that now. For those participants/patients who want to use an interactive dynamic system we're using computers. When you then call them back 8 months later because one of their choices becomes real so to speak that's when you, even if they have been clarified at the time of consent then you find out that they've already changed their mind again. But that's what dynamic consent is and that's perfectly valid.

DR. WAGNER: This, the exercise we're about to participate in is one where we need to hear sort of some last words from you. We are at the point in this particular effort where we are beginning to refine what will be final recommendations to the President.

And while I think each of us around the table may have taken one or two or five things from this morning's comments by you folks, we want to make sure that we are hearing from you the main point that you wanted to make.

So the question that started is what single issue, and we'll just run down the

table, do you think we need to consider as a Commission as we confront this issue of privacy and the public good in the context of whole genome sequencing.

And since Dr. Sweeney already put her pencil down maybe I'll go to her first.

DR. SWEENEY: That technology can help save privacy, that it can change your thinking, whether it's with respect to setting norms like the labs that we talked about, whether it's with respect to changing the way you set up the platform so that the platform can do more analysis on the platform versus sharing the data around. Or whether it's these teach-back consent forms. There is a technology developing around teach-back consent forms where you give the consent, you ask some questions. If they don't answer the questions properly then you provide some education and so forth. So I think technology can play a big role so that we're not necessarily trapped into --

DR. WAGNER: So the very thing that we imagine as threatening privacy we could be using better to help ensure it. Yes, I'm going to follow up with you later too because I like what you just said. Dr. Suter.

MS. SUTER: I think I would go to the importance of focusing on limiting uses that are detrimental which goes to the building of trust. And I know that -- I had thought about talking about the access versus use question in my presentation. The only thing I would add about that is I agree with Laura about the point about access. If there is some element of control that people need to have to be able to express certain kinds of preferences and in some cases it can be harmful to groups that you may be a part of. And so limiting access can be important.

I also think we want to think about access not just in the context of research in clinical settings but also access in other settings. So, even if we prohibit the sequencing of somebody's, you know, taking your cup and sequencing it there are other ways you can get genetic information. And if you're not a researcher, if you're not a clinician and you don't really have a reason to have that limiting access to those others, not just their uses but the access because sometimes it can be hard to prove that there were the nefarious uses. And so there have to be contexts I think where we limit access as well.

DR. WAGNER: Limit uses first, but also context in which -- limit uses --

MS. SUTER: Right.

DR. WAGNER: -- as a primary point you made. And your secondary point is we will find occasions where it'll be necessary also to limit access.

MS. SUTER: Yes.

DR. WAGNER: Thank you.

DR. KNOPPERS: Totally agree with the last point so I won't repeat it. I think citizens who participate in research expect their data and their tissues to be used so I would maximize use and access under the previous -- with certain safeguards but increase oversight so that the trust stays ongoing and is not breached. Because otherwise the data and tissues that they gave for research will never lead to improved healthcare. So you're on a contradictory route if you over-limit access and use. The very purpose for which people give their data and samples is for improved healthcare.

DR. WAGNER: Got it. Parsimony. Ken.

DR. CHAHINE: Yes, so I somewhat echoing -- I think trying to give as

much access with, you know, the reasonable limits that we've discussed I think is important. I think the reality is that, you know, the science and it's just going to need a lot of data, a lot of population data from a lot of different groups. And I think that really is going to lead to the hypothesis-generating research that ultimately is going to lead to improving health.

And I think, you know, we have identified a significant number of the, you know, if you will, easy wins in sort of genetics and I think it's just getting harder and harder every day. And I think we're going to be surprised at how much data we're going to need to tease out cause and effect going forward.

DR. WAGNER: I'm going to come back to you too.

(Laughter)

DR. WAGNER: Laura?

DR. RODRIGUEZ: So I agree with the things that have already been said and I guess I would add to it in the sense that clearly we all think that research is a good thing and there are a lot of public goods that will come from it. And so having that validated going forward is very useful, particularly in the context of the fact that we don't have all the answers right now and that it's okay to have some frameworks around which to move forward.

And to continue to ask our questions which comes back to what Bartha mentioned too is there are resource questions as well for the dynamic stewardship that I think is needed as we continue to move through this transition of new knowledge, new technology. And learning how to interpret and use that new knowledge and technology.

DR. WAGNER: If I might both -- keep your hands up. Thank you, if

you'd keep track.

DR. GUTMANN: I'll keep track.

DR. WAGNER: To both -- as much access as possible. Actually that's sort of the charge to the whole committee. Is access and ownership, or access and possession of data, access to and possession of data. Are they the same things? Do I actually have to possess those data and risk their further distribution in order to have sufficient scientific access for particular uses?

DR. CHAHINE: So I'm not sure. So you're saying do you need to have -- go ahead.

DR. SWEENEY: I'll go first and then you just clean up, how's that?

(Laughter)

DR. SWEENEY: No, actually you know, the idea of keeping the data in place is coming anyway through the examples I gave you of Facebook and Google for example. And I think it's a -- that we need to think about that with respect to research. And the way you do that is you build up richer environments for which computations can be done.

So like in dbGaP, you know, as you pointed out, that gee, people want these distributions on alleles and so forth. And then you're like, well, then what you might consider doing is pushing computation into the access so that people can do computations to get answers to distributions which don't have the sensitivity risk of actually providing individual --

DR. WAGNER: So it's about computational access.

DR. SWEENEY: Right.

DR. WAGNER: Not necessarily possession.

DR. SWEENEY: Right.

DR. WAGNER: Which I think we could do with greater security, don't you?

DR. CHAHINE: So, I absolutely agree. I think we're moving in that direction where you don't have to possess it to get useful information. I mean, the world is moving towards, you know, algorithms and the computation.

The one thing I would say is that currently full genome sequencing that's being done, a lot of the data that's being banked isn't, you know, fully sequenced, right? And so there is some need to have some possession for some time and probably arguably for reasons that we can't know today, right? That we'll want to go back and need the possession.

DR. WAGNER: And the panel agrees that's the highest risk of all this is too many people possessing when in fact computational access will someday or may -- all that needs to be sufficient. Raju was next on our list. Thank you.

DR. KUCHERLAPATI: I want to ask rather a broad question for all of you. And the question is how important is this issue from a citizenry point of view? So, I want to frame that and say that many people want to participate in research for either welfare of the whole population or the welfare of a subset of the population that have a particular disorder or whatever the case may be.

And the organizations that obtain certainly whole genome sequencing is

increasing rapidly. And we talked about some of the things like Personal Genome Project where people willingly want to be able to provide their information. People crowd-sourcing and want to be able to provide their information for the general good and so on and so forth.

So given this high level of interest in the public and many of them wanting to provide the data is the cat already out of the bag?

DR. RODRIGUEZ: So I'll start. For many it may be out of the bag. I think again we come back to the fact that it's very hard to make generalizations that work across the spectrum of the population. And so we need to have a way to have balance in that and to respect some of those different preferences that there may be because we also as a research community need to get used to the fact that there are patient-driven research objectives now and they are coming together to do this. And that's a different perspective from another angle. But I think we still have to be mindful of what the individual or group culture may have to do and not just decide it's done, this is reality and let's go forward.

DR. CHAHINE: So I think if I understood the question I do think that the consumer-driven nature of this is going to -- it's just going to move forward. It's hard for me to see a situation where this doesn't move forward and that's why, you know, I think that having sort of safeguards if you will sort of at that last point are important.

But as I said earlier, we're seeing customers either willingly giving up data or, you know, we have to contend with the password that's, you know, ABC123, right. But either way there's ways to get access and I think consumers really, we do hear that they want it, that there's a sense of ownership.

Whether there's a fear of how it's going to be used is almost different than

just it's mine. And so I really do feel like the momentum is going in that direction. I feel it and so I don't know that you want to call it the cat out of the bag, but I think it's moving in that direction.

DR. KNOPPERS: I think we have two parallel trends. We have the self-help trend which is exemplified by the direct-to-consumer, those who can pay can play so to speak. And then you have the larger systems where people want to have quality assurance when they go into hospitals and so they realize that a certain amount of information has to be available in the public domain in order to ensure safety and quality of care. And that's where their citizenship role kicks in in terms of them expecting that healthcare is based on quality data and to get quality data you need, as my neighbor said, tons of data. And to do that you have to act as a population. So there's self-help and there's group help.

DR. SWEENEY: Yes, I would say the question is is the cat out of the bag. There are lots of cats and lots of bags. So, you know, part of what you want to do, we're at that point in time with this problem. And so some of what you might want to do is set up new bags and see where cats go.

But the other thing that you have to do, what you're really trying to do is get ahead of a disruption. Because if you get a major disaster that happens and it shows up on the front page of the newspaper then in fact some outcome will happen immediately from Congress or wherever and you won't like it. And it won't necessarily be optimal or good. And I think what you're really trying to do is get ahead of a disruption to figure out which of these bags might be a real problem and which ones may show more promise.

DR. GUTMANN: Could I -- I just want to underline that, that in some

sense that's our job which is to make sure that we at least articulate the conditions which science for the public good can go forward without getting derailed by some incident that could have been prevented had only there been an articulated sense of what the constraints should be on this. Very well -- really well put.

DR. KNOPPERS: One brief comment. It has to be based on a reasonable expectation of a likely probability of its occurrence. Because you cannot build policy on what I call the unethical trump card of hypothetical situations, the worst case scenario in other words. My students always talk to me about Gattaca. I just open my mouth on genomics and there we go. And that is not the kind of scenario you want to build policy on.

DR. FARAHANY: Well, that's a nice segue way to my question which is since everybody seems to agree that it's at least primarily about use if not also somewhat about access, I really want to drill down a bit as to what are the uses we're afraid of or that we should be afraid of and to really get those out on the table. Because we talk about trust, we talk about privacy, we talk about, you know, whatever these hypothetical situations might be, something terrible happening on the New York Times, and yet without actually specifying what we should be concerned about I'm afraid that it's just kind of fear mongering rather than being specific. So I've heard a few and I'm just going to play out a couple. And I was hoping that each of you could add what, if any, additional things you think we should be concerned about. So, discrimination is kind of constantly on the table whether it's a Gattaca form of it, or employers, or health insurance companies, that's part of the motivation of GINA of course, and there may be other contexts for discrimination.

Reputational issues. So issues that might arise from the release of sensitive health information, from mental health issues, from even ancestry that people may not wish to have revealed. So it might be something like that.

I heard also that there may be some cultural beliefs or other beliefs about individuals who simply don't believe in the sharing of the information. I don't know what that is. I'm hoping that individuals who raised that could identify it.

That's what I have so far. I'm hoping we can build specific additional uses that we might be concerned about or should be concerned about to guide our discussions. So, I open that up to all of you and I hope that anyone who has a perspective on it will share what uses, if any, we should be concerned about.

DR. SWEENEY: I'll go first. A lot of my work -- I mean, usually when I get involved it's because somebody has a revenue stream they're trying to protect or they're trying to stop one and so forth. So we often, my work is often rooted in economic harms. And in the case of the genomic information that would be criminal and civil liabilities, things like that.

And then what's driving it often from the kinds of problems I usually get engaged in is money and somebody's making money. And then when it gets exposed or is made aware to the individual who might be the subject of the data they had absolutely no expectation that this could happen or would be used or how that person even got the data.

And you know, just a very simple example of that would be, you know, you hear that somebody had a breach of credit cards, of Social Security Numbers and you've never heard of the company. Why in the world would you believe they had yours, but yet

they had your data. And you're trying to figure out how did they get it, why did they get it. And it's because some of the notices that you received said oh, we sent it to this kind of data. Or a lot of attention is paid on the data use agreement when the person first got the data but not downstream uses of the data.

DR. KNOPPERS: There are three categories, discrimination/de-stigmatization we can throw in there, cultural/origins and reputational are the classical generic objections or fears of leaving it open so to speak and seeing what the marketplace can bring. And our laws that already exist are there to protect us, constitutions and otherwise.

I think the biggest threat of genomics or genetics -- and I don't believe in exceptionalism, like my colleague to the left I think it's sensitive medical information, that's all -- is that because of the genes and the genealogy and all the archetypes that come with it, that you are already perceived.

It's not having something that's the difference. You know it if you have it. Your family knows it, your ethnic group knows it, your whatever. It's being perceived as already ill. It's being perceived as coming from the wrong tribe so to speak or having different origins or being associated with a gene for some sort of intellectual disability and so on. So it's the societal interpretations of the genetic information that already makes you be seen and treated as if you were whatever that is. And that's where it is. That to me is the threat.

MS. SUTER: Can I add to that? So I think there isn't really a new category, but in the context of discrimination you talked about employer/insurer. I think

one good example about what Bartha's talking about is in the situation of education where we make a lot of presumptions about what people are capable of or could based on this information. And so I think that the discrimination could be seen as including many more categories than just insurance, employer. Also concerns in the adoption context. There are a lot of other areas where discrimination might be an issue here.

DR. CHAHINE: I would just say, and I'll give you maybe a little bit of data from Ancestry. But I feel like, you know, maybe I'm being naive or too hopeful but that the genetics is going to be an equalizer in some ways. And I feel like yes, maybe I'm being hopeful.

DR. GUTMANN: History suggests you are being hopeful.

DR. CHAHINE: That I'm being hopeful.

DR. GUTMANN: It could be used either way.

DR. CHAHINE: No, it certainly could be used either way, there's no question. And we've seen things already with, I believe it was in Hungary or that one group that was looking at sort of genetics, at their political figures.

But I would say, you know, Ancestry, the vast majority of people leave their family trees open and they have that choice because they want to collaborate and their goal is to basically continue to learn more about their genealogy.

And I think, you know, even in genetics, I mean we do take for example our ethnicity and matching. We keep it closed so that the individual has the right to open it up or not. We're still too early to determine how many people are going to make it completely open. But I can say we don't -- we don't hide the ethnicities that we come up

with.

And so there are people every day that are learning that they are X percent, you know, African that maybe didn't know it before. And that's happening every day. We're also seeing other ethnicities. And I'll be honest, you know, we have not heard any sort of negative -- I haven't heard a single negative complaint one way or another.

And I think, you know, I'm hoping that maybe I am hopeful but I do hope that data like this takes us away from these gross phenotypic differences that we have relied on and all of a sudden give us a different perspective of what it means to have different ethnicities and different, you know, races. And I hope those terms just sort of disappear because they become meaningless. And so those are my --

DR. GUTMANN: That's a wonderful possibility and I think it's part of what you're doing, but Nita's question what was are we, you know, what are some of the things we're -- people could fear. And let me just add to your list because it's a good list to accumulate. If we're identifying, you know, identifying people, people might fear that it will become public knowledge even before they know it that they're related to some nefarious person in history. They're related to Hitler or Stalin or, you know, we're talking about the fears now.

There's also a generalized concern, I wouldn't even call it a fear, but a concern that there will be invasion of one's privacy without one's consent. That is, knowledge about one's self that one doesn't want to share publicly. Some people aren't concerned about that at all and other people are.

So, there is a fear that because we're living in an age of Facebook and

Google and a billion people are -- I'm rounding to the nearest billion, a billion people are Facebook that the billion people who now don't want to be and don't want information about their lives that publicly shared will be forced into that world. So there's a concern about invasion of privacy without one's consent because the vast majority may or a plurality may want it. So those are concerns. They're not necessarily trumping concerns, but they're concerns that are there.

DR. WAGNER: Did you have a follow-up?

DR. FARAHANY: I do have a follow-up which is so first I think that's helpful, right, to think about it as some people are concerned about the information getting out there. I would -- I question whether that's an invasion of privacy or if it is a concern an individual has. I think that's making a judgment that it is an invasion of privacy whereas part of what I'm trying to get at is understanding what is the concern about having information shared.

You've articulated a really helpful one which is some people don't want information out there before they even know it themselves and some people wish to actually create a personality that they don't share with others. Yes.

DR. GUTMANN: So Nita, but let's -- I want to clear this up because Nita has consistently not liked the notion of, you know --

DR. FARAHANY: No, I like privacy, I just, I have a different conception of what it means in this context.

DR. GUTMANN: Okay, well -- so if you look at the concerns in Rachel's piece one of them is that in order to have relationships of various kinds with people we

share different levels of information with them. And a whole genome sequence gives a lot of -- it's not -- you could aggregate this information in lots of other ways but it gives a lot of information about your person, perspective as well as. And there are people who legitimately see some of that information as private information that they don't want to share without their consent.

And as you recognized earlier, one of the reasons that someone, you know, shouldn't just pick up a coffee cup and pretend they're you and get this sequenced and put it on the web, one of the reasons is you should have some say over what -- how many people and who know this and for what purposes.

DR. FARAHANY: I agree. The "some" is the only thing I'm pushing on, right? Which is it's not -- I don't believe that all of the information that is contained necessarily would make a person violated. As to trying to get at what uses people would find concerning, I think tries to articulate the difference between what might actually make an individual feel violated versus what information is actually something we don't have an expectation of privacy around.

MS. SUTER: Can I -- at the risk of belaboring the point. I do think that talking about the harmful uses is a really important way of thinking about privacy, but I think privacy can't just be about harmful uses. I think that there is intrinsic value. I think the racial piece you were talking about many others have talked about. The sort of formation of the self, how we understand ourselves, how we build relationships, I think privacy has a strong relational component. And so I think that has to be understood as part of privacy.

Now, whether we give it as much weight as the other sorts of harms I think is a different question. But to me that seems very much a part of how we think about building some sense of the self. And intimacy and relationships with other people.

DR. WAGNER: I think that's a very good point. I will add though, back on the harmful side we've heard again from Dr. Gabriele. I just want to read this into the record.

He suggests a good word for much of what we're talking about if not another piece on the list is a concern about exploitation from having these data out there. I think it's a good word.

DR. CHAHINE: I'm sorry, so the exploitation in terms of certain individuals? I'm sorry, I just wanted clarification in terms of exploitation of certain classes if you will.

DR. WAGNER: Well, why don't we have Dr. Gabriele stand up and mention that. Yes. Holler for us.

DR. GABRIELE: Thank you. One of the things that I find when we -- I work a lot with healthcare ethics and as well as human research. When we talk about exploitation I'd rather not limit it. I think that's part of the problem. Exploitation, the fear of exploitation is a fundamental fear to the human animal. I'm scared to death of being used and abused. I think if we've worked in counseling with folks who have suffered from abuse we know that.

So when I come forward and someone says that they're going to take my data and use it in whatever way there's a thing that happens to me psychologically,

spiritually if you will, emotionally and that's a problem that's talked very much in history in the work of Nicholas Berdyaev in moral objectification. And I think that there's a need to revisit some of those good conversations and dialogues that have happened over the last 100 years about that, especially in the light of the Holocaust, Tuskegee, Guatemala, Nigeria, Jesse Gelsinger, Ellen Roche, and we take a look at what do all those things have in common - exploitation. When I am no longer a patient, I'm now a customer, or worse, the generator of relative value units in electronic medical record system. There's a sense of depersonalization that I think has to be looked at.

DR. WAGNER: Thank you. Dan, let's go to you.

DR. SULMASY: Yes, I very much appreciated the analogy to the Tower of Babel and think that maybe one of the things the Commission might do is to help clarifying language.

And we've just had some discussion about that, about the question of privacy and its scope, whether it's not just harm, not just a question of ownership, but the sense that genomic information is if you will not just knowledge about me but knowledge of me, that it's embodied information in a way that's not absolutely unique but important as a difference that's contained perhaps under privacy.

Another set of things that we might look at I thought, clarifying definitions and relations between terms like privacy, confidentiality, anonymity and trust. To think about for instance confidentiality as privacy in trust. And if we have all of those things lined up we might be able to help clarify the literature that way.

Or Jim has mentioned several times access, possession and use. Related

but different, how do they relate to each other. And so it seems to me that there's a lot of conceptual work from what I've read that needs to be done, that this Commission might do well but maybe I'm wrong.

Maybe this is all out there already clear in the literature so I'd like to hear from you if that is the case so we don't have to waste our time. We'll just cite somebody. But if it is useful tell us and if it is useful also tell us if there are other areas besides the ones that I mentioned.

DR. WAGNER: Run through your list one more time. You were talking confidentiality. Was secrecy in there? Was that another piece?

DR. SULMASY: I'll keep secrecy in there too I guess, yes. But this sphere of sort of privacy, confidentiality, trust, anonymity, secrecy which are all related but distinct and have distinct roles here in these sorts of discussions.

DR. WAGNER: Good, good. Thank you.

DR. KNOPPERS: I think those trios are really helpful because they show within a range depending on what relationship you're in which one becomes the most important, or which one should be protected by the state and which one is a personal decision.

With whole genome sequencing you get sort of three levels that have to be distinguished as well while we're on trilogies. You get the filial, you get the origin stuff, you get the biology which is maybe the more sensitive than the -- what I would call the Mendelian genetics ones. The rare mutations, though most people would probably know because those rare mutations run in families, but still, those are the fateful ones, the ones we

associate with disease and horrible outcomes. So that's also very sensitive because it affects your whole life, your family life.

But 90 percent of what we're going to see in whole genome sequencing is going to be probabilistic indecipherable information. And my only hope, and maybe I'm an idealist like my neighbor on the right here, is that we're going to discuss like we do the weather and airplanes that don't leave, we're going to discuss I'm at risk for this, yes, but my brother found these, and my aunt, but my friend down the street, can you believe. So we'll be talking about it like the weather and the probabilities are about the same.

(Laughter)

DR. KNOPPERS: And that will equalize. In other words, we won't be equal but we'll be equivalent in risk. And that's what I think is what NGS, next generation sequencing, will make us learn how to live with.

DR. SWEENEY: Yes. I was going to say that I think that vision of being able to move society where we can talk about personal genomics like weather is a really good one. But to get there this interplay between privacy, confidentiality, trust, anonymity and secrecy is really interesting.

I'll give you one example that I heard in the second panel is the use of the data use agreement and the word "de-identified." So, if -- I applaud the work of NIH and many homages to NIH, but -- and I don't mean to pick on NIH because this is a very common thing we see whenever the government is involved in the data is this heavy use on this data use agreement and heavy use on the reliance of the word "de-identified." So to the extent that if you say de-identified doesn't really carry strength then why use that word in

your presentation? Because in fact a lot of the protections did not assume that de-identification was strong. But it's a loaded word because to those who want to believe in de-identification it means anonymity and therefore the data is less risky. And the absence of the word means fully identified or almost identified or leaving it open and people -- it sets the barometer. So, that's a real problem.

In both the Ancestry data, our own experiments, our own published results as well as the GWAS study show that data can be re-identified. A very simple example is trinucleotide repeats. So, like Huntington's disease, we were able to show that if you have the genomic sequence the length of the repeat will tell you the age of onset. You go to hospital discharge data that's publicly available and you'll see an estimate on the age of onset. You'll see where the person has gone. You'll get demographics and then you relate the demographics to a population registry to put back a name. So, and there are other -- and others have shown other kinds of vulnerabilities.

But rather than run the other way in a data use agreement by saying it's de-identified and by the way everyone's guaranteeing that they won't identify participants I would push back on that also against this I won't re-identify. Because when you say -- when there's a lot of money involved and the group that got the data said that they would not re-identify people, what that really means in practice I can tell you on the ground is you re-identify because you have a reason to do that, but you just make sure nobody ever finds out that's how you got that data.

And so as a result -- and it also squashes experiments. It makes it very difficult for those of us who want to say where are the risks and what are remedies in

identification, it squashes our ability to actually say to NIH this is a risk and here's a remedy to that risk. Because after all they won't -- you can't have their data if you're going to re-identify.

So I give that as an example of how the role of anonymity relates to trust, relates to confidentiality. So what you guys are dealing with is not just the definitions of these things but the ecosystem of interplay between them.

DR. CHAHINE: Just one comment. It was interesting coming from sort of the science into now the internet world where we have to communicate the genetic findings to individuals is boy, there's a real chasm there, right, in terms of the discussion here today and how that's going to be communicated. And I think we work very hard every day to make sure people understand simple genetic findings. You know, up until a year ago everything was a haplotype and I'd have to go and figure out, like, where does that haplotype live. And then, you know, the reality is people were turned off by that.

When we asked people do you understand the results like 75 percent said I have no idea what you're talking about, and that was the simple haplotype that you could plug into Wikipedia and find out the region it came from. So, imagine these issues. So I think we just can't lose sight of the fact that at the end of the day it's a customer and we need to really boil this down to something super simple that they understand.

DR. RODRIGUEZ: I'm sorry, could I just -- that's okay. I just wanted to respond a bit to Dr. Sweeney's comments. And not in a defensive mode but because I think it's a way, an area that the Commission might be helpful in thinking about or talking about this going forward with the kinds of conceptual issues that we're dealing with.

A lot of the reason that we are bound and talk about in our structures the de-identification issue is because we are bound very much in setting up any of our agreements to promote trust by existing law. And that's how things are defined at the moment. And so the science and the technology has moved past our existing laws and regulations and we are trying to create new systems or adjust systems with what we have in hand. And I think some new perspectives on that that you all might be able to define through this conceptual work would be very helpful and could then inform new adaptations to bring about the trust that we're seeking.

DR. MICHAEL: Dr. Chahine asked -- during his presentation mentioned the safeguards against data breaches, and mentioned that you actually run drills against people probably as good with computers as my 17-year-old to be able to potentially get access obviously when that was unintended.

And so I guess my question is I understand my own agency that I work with is very interested in information assurance as you might imagine. I know that the NIH is also intensely interested in the security of its information systems. Obviously you have fiduciary concerns to both your clients as well as your shareholders for Ancestry.

So what lessons are shared? Is there a process between public and private database holders so that lessons about what threats there are to security for databases are shared across public groups like the National Institutes of Health as well as private industry or academia.

And I ask this question because all of us are talking about some of the nuances that may occur to what we define as the real threats to privacy. But obviously some

of these explosive situations where if your database or the NIH's database were to be broken into, that would I think again probably trigger as Dr. Sweeney said some very quick and perhaps sledgehammer approaches from regulatory or law-making authorities certainly in this country that I think may put a pall in the whole enterprise.

So is there a sense across the community that sits here on this table about how you could collaborate to share what you understand about information assurance and basically make the databases more resilient?

DR. CHAHINE: So let me respond to the question. Are we as a corporate institution willing to sort of work with others in terms of what we've learned in terms of security for example, is that --

DR. MICHAEL: Yes.

DR. CHAHINE: Yes, absolutely. We feel, you know, we're still sort of developing our own policies. I mean, we're generating a lot of data and have, you know, increasing amounts of genetic material. We're trying to figure out the best way to collaborate.

I know Laura and I have talked and we continue to work with NHGRI to kind of figure out what that best -- the best way to do that is. Because we do believe even from a corporate perspective, right, the models are changing. And sort of keeping everything tightly to yourself isn't always the best way even from a commercial standpoint. So we're also in sort of a shifting model here.

And in terms of privacy I think absolutely. I think the lessons that we've drawn from are, you know, a lot of the credit card and other things that we've worked on.

And so we've drawn from that. We're more than happy to share. But at the end of the day let's, you know, to be very candid it's layers of security, right? That's what it comes down to. So that it just makes it increasingly harder to continue to breach.

And we're just about to put a tokenization system that adds yet another layer. And you know, that's as good as we've been able to get it.

DR. RODRIGUEZ: So and I would just concur with Ken in the sense that we're actively looking to all other partners to try to find out how to do this better.

And so in the area of cloud computing, for instance, where the private sector is far ahead of where the government is and how to work with it and how to fit it within our environment. You know, we at NHGRI held a workshop 2 years ago to bring all of those providers in to ask them, you know, what are the issues and then talk to them about the scientific needs.

Because there's a communication and a dialogue that needs to happen in both directions so that you can take the kinds of computational access that we're trying to think about and figure out how do we make it work in the different environments in ways that still retain the security that they may have developed for their purposes.

DR. KNOPPERS: In the large international projects where up till very recently huge amounts of data were shared under very tight conditions, we're seeing an end to that not only because we can no longer handle the amount of data that's needed internationally and make sure that it's secure, but also because of the kinds of data, whole genome sequencing totally changing the pattern of what --

DR. WAGNER: I'm sorry, seeing an end to what? An end to

collaboration?

DR. KNOPPERS: An end, no, not to collaboration, to how we share data. And so we're starting to work on different algorithms which I think you also brought up. So we have mathematical models that we're piloting right now in different projects such as BioSHaRE and the FP7 project in Europe where we're actually sharing very rich phenotypic data but it never actually leaves its real location. But through the algorithms you can actually share it with other countries and other individuals. You don't have to ship the data, the raw data per se.

DR. SWEENEY: I just wanted to address this question about information assurance. It gives us yet another trilogy. That would be security, privacy and risk-benefit tradeoffs. So, in this conversation as often happens when you're not actually having the computer person who has to be responsible for these problems you tend to merge security and privacy, but they're actually radically different.

So security has to do with have the data in a repository, somebody broke in. So this -- and how do I make sure that when they broke in they couldn't get anything useful or they couldn't get in at all.

And then privacy has to do -- this notion of privacy anyway has to do with I gave this data away. What is the risk to the individual or to us, the organization, for having given or shared this data in this form.

And so these are different kinds of threat models. They both though have this idea of risk-benefit analysis. So you know, it's sort of like what she was saying earlier, it's how likely is it to occur. If it did occur, how bad would the impact be and how much is

the cost or the remedy for a solution.

And one of the best examples -- the problem with it, it makes it very difficult once you set up a database to talk openly about these kinds of security threats or these kinds of privacy risks if they're likely to happen and have an adverse impact.

And even if they're likely to happen and have an adverse impact and you know about it and you know a solution but the solution is expensive it's hard to make it go.

And so what we've seen historically in the financial area is it didn't get addressed. And so that was one of the brilliant pieces of the breach notification laws because all of a sudden all these breaches were happening. Well, you know what? Those breaches were happening anyway, but now it's -- you change the risk-benefit because it's better for them to let you know so they don't get hit with a lot of penalties than to keep it secret. And of course that has improved the security models in a lot of these systems.

DR. ALLEN: Well, when I first raised my hand I had one set of thoughts - - so much very, very beneficial discussion. I'll just kind of run through my questions and concerns.

As for the list that Nita Farahany began to generate about what the fears are I think, right, discrimination, reputational concerns, cultural origin concerns. And then we added to that problems about profiling and categorizing, putting people in boxes. I heard the word identity theft. I heard concerns about being forced into social networking contexts and invasions of privacy without consent being its own sort of concern.

And I just wanted to put a fine little point here on this concern about commercial exploitation because one specific type of commercial exploitation that I know

some people are concerned about is the sort of concern that was raised by the development of the African-American targeted drug BiDil, the drug for African-American cardiac disease where what could have been seen as a public good, namely an effective remedy for a condition, was seen instead as some way of profiling, discriminating, exploiting people. And so as we make our list of what people are afraid of we're going to have -- some of the things they're afraid of are going to be sort of oddly intentioned with what we might think of as public goods. So that's just one sort of point.

I also wanted to comment on the issue of trust because this has come up again and again and again today and I found myself thinking about the work of one of my mentors, the very pioneering ethicist Sissela Bok who described trust as a fragile good. And it is a very fragile good. It's fragile because on the one hand it's something which we often say has to be earned, right? On the other hand, we know that trust comes with the territory. The people in the white coats get it automatically from some people. So, you know, in thinking --

(Laughter)

DR. ALLEN: -- in thinking about trust we need to constantly remember that it has this sort of odd dual dimension of having to be earned and yet coming with the territory. And it may well be that if we're going to kind of loosen or lessen our privacy strictures based on building trust we have to remember that it's easily lost and easily broken and it has this kind of funny way that it comes about in the first place.

And then finally, discussion turned to what kinds of conceptions of privacy are we talking about anyway. What's the relationship between privacy and anonymity, de-

identification, confidentiality and secrecy, and in trust. And you know, I think that it's easy to get bogged down in what all these terms mean. But there's a vast and I think quite good literature going back now to nineteen seventies and eighties that attempts to sort things out.

And I think a lot of us today, I mean, you know, your colleague Dan Solove and I both have in our work quite independently described privacy as an umbrella concept. You know, it's a little bit vague but it's just a broad general concept that encompasses anonymity, confidentiality, secrecy.

Well, how so? Well, the way I would put it in my own work is that -- learning a lot from, again, Sissela Bok and others, secrecy involves intentional concealment. That's a unique little conceptual there around that is it's intentional concealment. Anonymity has to do with concealment of personal identifiers. Confidentiality has to do with limiting access to data to authorized recipients of that data. So each of these terms has its own little set of sub-connotations.

But I think what they all have in common under this privacy umbrella is the idea that we're trying to create conditions that limit access to information and to people. So we're limiting access to personal information. That's what all these things have in common.

And so if we're talking about doing it intentionally we might be talking about secrecy or about anonymity. We're talking about who's authorized to know, we turn to the confidentiality discourse. But I don't think we need to sort of feel like we're in an escapable muddle just because these concepts do have their own unique uses and yet they're sometimes conflated.

MS. SUTER: Well, and I just want to add to that and then property may or may not be included in part of that as well.

DR. ALLEN: Yes.

MS. SUTER: I mean, property itself is a really complicated term that can mean all sorts of different things. And you know, the bundle of different kinds of rights. But I mean property can fit in there. I personally find it problematic to think about the privacy norms in property terms, but plenty of people want to think about it that way and have tried to.

DR. ALLEN: Yes.

DR. KUCHERLAPATI: I wanted to pose a question to Bartha but I would also like to have views from the rest of the panel members.

So Bartha, in your last slide and the first recommendation is that not regulations but guidelines. And maybe you could articulate a little bit more as to why you think, you know, that approach is better than regulations. Is it because of the dynamicism of, you know, where things are going? I'd love to hear.

And I'd also like to hear from the rest of the panel whether they share your view that guidelines are a better approach than regulations.

DR. KNOPPERS: I'll go in reverse. Guidelines are not necessarily better, but I find that they make people think. Regulations are usually adopted pursuant to a law, that's why they're a regulation, not a law, and they tend to lead to both researchers and IRBs checking off whether they've met the fed regs this or the HIPAA 123 to 18. And they don't think.

And when you're dealing with people and complex issues and their values as well, never mind the context and so on, you have to encourage thinking both on the part of participants but also researchers and the IRBs and guidelines give you that latitude and at the same time the horror of having conflicting interpretations sometimes of the same guideline. But that's what distinguishes us from machines is that we have that responsibility to constantly rethink what we're doing and why, and guidelines encourage that.

DR. RODRIGUEZ: And I would just join in on that. I think regulations tend to become and be useful for addressing absolutes, but there are limited situations particularly in these emerging areas where we know absolutely what is the right way to go.

And guidelines can accommodate the complexity of reality and of changing situations, and they can accommodate change. And again, I think that's very helpful right now where we are all learning about this information, about how we will use it, about what it means and about how the public is going to uptake this information and integrate it into their lives.

DR. GUTMANN: Yes, I want to make an observation which I hope there will be agreement on but we'll see.

I think it's important for us as a Commission and for all of us not to speak about what -- just about what the fears are here. I think it's what do people, what do various people care about in this. And the reason I think it's important to talk about what we care about is because that puts on a level playing field the fact, and it is a fact, that I care about having whole genome sequencing being able to be used for the public good and for benefits, and I also care about it not being used for discriminatory purposes. Neither of these is a

fear. I mean there are good reasons to care about both of those.

I care about privacy in the way Anita speaks about it because I recognize and there's a vast literature here and evidence that one needs some domains of that if one wants them. If you don't want them you don't need them, you don't need to have them, but one needs them to discriminate in a good sense among relationships that one has. One -- I care about reputational risk, not just my own but other people.

At the same level as I care about having the ability of really good science to go forward, of people being able to see how they're related to other people and that can open up worlds of non-discrimination to them. And if we can use that, if we can understand that these are reasonable cares and concerns about people then as a Commission we can come to some understanding about how best to move forward with the science and what the science can give to individuals and humanity at the same time as protecting to the extent possible these other cares that people have.

DR. WAGNER: Tell you what. I think we'll let that be the last word. It has been a productive and informative morning and we have you folks to thank very much for that. So thank you.

(Applause)

DR. WAGNER: I believe we need to move with dispatch actually.

DR. GUTMANN: Yes, we're adjourned for lunch as I hope everybody will take the opportunity to nourish their bodies as well as their souls. And we will reconvene at 1:15.