Transcript of Statewide IT 2012

[Note that the actual debate begins on page 4. — Editor]

[music]

Brian: But nice dress.

Daphne: Thank you. Good morning everyone. Welcome to Statewide IT 2012. We're really excited...really, again, with the cane thing? We discussed that in rehearsal.

Brian: Wow, someone's cranky. Did you lose another sheep?

Daphne: As I was saying before Mr. Peanut so rudely interrupted me, welcome to Statewide IT 2012. We're really excited to have you here today. This is the largest Statewide IT ever. We nearly double...what?

Brian: Attendance from last year, yes.

Daphne: What now?

Brian: Oh, yes, sorry. Look.

Daphne: What?

Brian: What are they wearing?

Daphne: Oh, no. Someone clearly didn't get the telegram.

Brian: Not at all. This is wrong.

Daphne: We told you this was a Lincoln-Douglas style debate. You guys must all feel completely ridiculous not being dressed properly at all.

Brian: Look at that.

Daphne: Oh, scandal! I see Deb Allmeier's ankles. Oh, this crowd clearly has no decorum left.

Brian: No, none at all. So since you didn't come appropriately dressed, I can only assume that you brought a bunch of noisy, annoying noise-making devices. [audience cheers]

Brian: That's just rude.

Daphne: Yes. Ever since they invented the mobile telegraph device, all I hear at every conference is clicking and clacking.

Brian: And "Battle Hymn of the Republic" ring tones. I used to like that song.

Daphne: I know. I'm so over it. But anyway, please be courteous. Silence your mobile telegraph machines now.

Brian: Yes, but don't put them away because you might want to use them later. If you want, you can tweet. You can tap your tweets to #SWITC or you can talk directly to Roxy at Statewide IT.

Daphne: Yeah, so for those of you who don't know us, I'm Daphne and this is Brian. Together, we lead the IT communications office. And this year, we are also the general chairs of Statewide IT 2012. But that doesn't mean we deserve...

Brian: All the credit.

Daphne: ...much or any of the credit, really. There were a lot of people in this audience who deserve much more of the credit than we do for making this conference a success. So before we go any further, I'd like to ask that those people who are involved in the committee, who served as reviewers and track chairs, please stand up for just a moment and let's give them a round of applause.

Brian: If you helped, stand up, please.

Daphne: Yeah, please. [applause]

Brian: So immediately after the debate, we'll have a 30 minute break where you can go out into the foyer. We'll have break service again. We'll have some breakfast and some drinks. We'd like to invite you to visit our vendors out there again. Before you come back in here, make sure you stop by them. If you didn't pick up any pens or posters, you can get that while you're out there. And then we'll be right back in here at 10:30 for Brad Wheeler's annual keynote.

Daphne: After Brad's keynote, we'll be moving up the street to the IMU. And I'd like to stop for just a moment to say a couple of things about lunch. As I said, we nearly doubled attendance this year, and we have a lot more people. We expect a lot more people at the lunches, so we will take a little bit of time to get everybody through the buffet lines. So we're just going to ask everybody to be a little bit patient. And for those of you who aren't good at being patient, -- I know there's one or two of you out there -- we do have another option. There will be some box lunches available in the lobby of the auditorium on the way out here. If you are more of a box lunch type, go ahead and grab a box lunch. Meet us back at the auditorium at 1:30 for the breakout sessions.

Brian: We do anticipate that some of the breakout sessions may fill up this year, so try to arrive early if there is one that you're particularly interested in. If you get to one and it's full, don't worry. We're recording all of them this year, and they'll be posted to the Statewide website about two weeks after.

Daphne: So I see there are some people in the front rows here that are a little excited about the debate. [audience cheering]

Brian: I think they're rude.

Daphne: All right, settle down. We'll get to the debate in just a moment. But first, did you guys know that there's actually nothing in U.S. law that says that presidential candidates have to debate each other?

Brian: In fact, campaigning was uncommon in the past. It was actually frowned upon.

Daphne: It was really the Lincoln-Douglas debates that broke the mold.

Brian: It wasn't until 1858 that they actually broke the mold and got into political debates. And that's when Lincoln challenged Douglas to a debate for the Illinois State Senate, but Lincoln was initially turned down by Douglas.

Daphne: So Lincoln decided to give Douglas a little encouragement in a very "Lincolnesque" sort of way. He actually followed Douglas around the state where he was giving speeches, sat up in the front row and shouted heckles and retorts at him. [laughter]

Daphne: He did this about seven or eight different talks in a row. Finally, as the crowds grew larger and larger at every talk, Douglas decided that he should just give in and agreed to a series of seven formal debates.

Brian: At those seven debates, tens of thousands of people traveled around the state to see these talks, but none of them could actually vote for either candidate.

Daphne: So none of them could actually vote for the candidates?

Brian: No. At that time in Illinois, the senators were chose by the state legislature and not by popular vote.

Daphne: So if they couldn't actually vote for the candidates, why did they show up?

Brian: Much like the people today, a debate is entertaining and it's fun. Lincoln was a funny guy and Douglas would quip back at him, so people would come to see that. But on top of that there was a very serious issue at the time. They were primarily debating slavery, and it was something that was really morally challenging to the country.

Daphne: We won't be talking about anything quite as serious as slavery today.

Brian: No.

Daphne: But it's still serious.

Brian: Yeah. Today we're here to talk about cloud security, which is not quite as serious, but it's still something we should consider as we put more of our files online and more of our personal information into the cloud. We need to ask the question of what should we be concerned with?

Daphne: Or should we be concerned at all? To help us answer these questions and to form our own opinions on these matters, we'd first like to welcome the moderator of today's debate, our very own Vice President for Information Technology and CIO, Brad Wheeler. [applause]

The Great Cloud Debate

[music]

Brad Wheeler: Welcome, welcome to the great cloud debate. Someone may need some fashion consulting, I can see, afterwards, referring to our host. Debates are a really important part of our history, as Brian and Daphne shared. There's no doubt that this topic of cloud is hugely important. The New York Times, yesterday and today, have a multi-part series on where we are going with cloud. So with that we're very pleased to have two very distinguished debaters and spiritual leaders of the Cloud Now and Cloud How party. Let me first introduce Shel Waggener.

[applause]

Brad: Shel comes to Higher Ed as the former Chief Information Officer for a division of networking at Lucent Technologies. He was the CIO at Berkeley. Upon becoming the CIO there, he immediately rose to the head of the class with national influence over many things going on in higher education. Most recently, he was appointed as the Senior Vice President at Internet2, in charge of a cloud initiative there called Net+ Services. Shel is the spiritual leader of the Cloud Now party. [applause]

Brad: Mr. Wagner is matched by distinguished Professor Fred Cate, here of Indiana University. [applause]

Brad: Professor Cate is one of the best known, one of. This happens with Professor Cate. Professor Cate is one of the best known national speakers and voices on privacy. You'll see him quoted all over the nation. He serves on a number of national advisory boards, including those with the White House, with the Department of Defense, with the National Academies for Professors. He is frequently writing about privacy and is a local hometown favorite. Some of you will recall Professor Cate from last year.

Gentlemen, welcome.

[applause]

Brad: So, as we get started, let me just momentarily remind you of the rules of the debate. Each of you will be given four minutes to make your opening statement. After that, I will lead with a question to one of you and you will have two minutes to respond. Our trusty timer, here, is visible. And you have monitors to watch the time. I will monitor the time, knowing each of you.

[laughter]

Brad: You will have two minutes to respond to my question and your colleague will have two minutes to give a rebuttal following that. If you happen to say something substantive, then there will be a three minute period to follow up where you may engage each other. With that, the first opening remarks goes to the spiritual leader of the Cloud Now Party, Mr. Wagner.

[applause]

Shel Waggener: Let me just bring my notes up here for a second. Distinguished Professor Cate, as a member of the Academy, you of all people know what it's like to live in the clouds.

[laughter]

Shel: There's opportunity, there's advancement, there's creativity, all the things that have been brought forth through the evolution in technology that has happened over the last 50 years, we have seen, time and time again, huge leaps occur when abstraction occurs and pieces get moved further and further away from the individual technologist. We can have benefits from Moore's law. We can see components get smaller, get faster, become more accessible to all. In doing so, we have been able to drive the cost down and the benefits up, and make them available to the masses.

You would have us believe that staying out of the cloud is a safer way to go. Perhaps you still run a main frame at home, and you have your cloud based deck of cards to feed into that machine, to tell it what to do.

Whereas I have more power in my hand than every computer built from 1950 to 1980 could have had, available to any one institution, I now have available as a single individual. That's because of the cloud. Not because we each run our own systems. I know as a server hugger you would prefer to keep those close to yourself. I understand the importance to you of the blinky lights and making sure that you know that they're safe because you can see them turning on and off.

I, however, rely on open standards, community involvement, cloud security alliance, NIST and federal standards, and more importantly the global engagement in computing, to help ensure that we continue to see evolution and don't simply stagnate. Running our own machines in our broom closets at home.

That said, I know there are, in fact, benefits to doing so in a place like Indiana where you do need to keep warm certain months of the year and when you do choose to write your own software, writing the 350th version of an application just so you can have written the code yourself does make a lot of sense.

If you choose to make it secure, that is until one of your graduate students hacks it in about five minutes.

The cloud represents a $250 billion market. $250 billion in investment means an investment in security that will eclipse anything, anyone individual or institution or state can accomplish on its own.

That level of investment dwarfs all that have come before it, and represents not just an opportunity in the education space or for any of us individually, but in fact, for all industries and all communities to be and to collaborate in new ways.

We have seen some of the greatest advancements in software come from open source and community source development. The cloud offers an opportunity to take those collaborative activities and expand them far beyond any one institution or individual.

Look at the impact and benefit of the Linux environment, and what happened as a result. Whether you chose to proprietary software, running locally or open source software running locally, in both cases both the ecosystems benefited because of the existing of the other and a competition that resulted.

The cloud represents the next evolution in that opportunity. Besides, who really wants to carry around your eight track tapes anymore.

Thank you.

[audience cheering]

Brad: Professor Cate, four minutes.

Professor Fred Cate: Thank you. Distinguished carpetbagger from California. I was reminded as we listened to your talk about the value of this technology you're so found of that we're looking at digital timers that have said 0:00 throughout the entire talk.

[laughter]

Fred: Simply anticipating the value of your conversation today. Or as Lincoln said to Douglas in the original debate, "Your argument is thin as the homeopathic soup boiling the shadow of a pigeon that had starved to death." Here's the great idea you're trying to sell us on. Let's take our most critical data, our single most valuable asset, and the applications we apply to those data, and let's move them away from our facilities, away from our oversight, out of the control of the people in this audience who normally run them.

And instead, let's put them some place far away. How far? We don't know. We don't know where they are. We don't know where they're located. All we know is, we have intermingled them with data from dozens, hundreds of other organizations about whom we also know nothing. And then let's put them in a cloud on which we draw a target.

And say, "This holds the most valuable resources of our modern economy." Subject to attack from anywhere. Subject to the government controls of any country. In fact, let's make sure that we take those data and, instead of empowering IT professionals to protect them let's empower lawyers, lots of lawyers. Lawyers need jobs.

[laughter]

Fred: So that we can spend the next decade negotiating over the contracts of where the liability is going to lay when this data are compromised which they inevitably will be. In fact, having given away possession and control of our most viable assets and having fired these people to replace them with a team of lawyers who can work throughout the night making sure that liability will fall to the right place when bad things happen. Let's then give all of this information to our loan provider with a long history of security vulnerabilities. What's better, let's create a new provider with no history whatsoever. Let's give them control and then what we'll do is we'll pay ever-escalating fees in exchange for the services that they're going to provide. In cloud computing, I have to say, we are fooling ourselves.

Not that cloud computing will never be appropriate. Not that there are no services that could be put in the cloud. But the notion that we are going to transfer away from us, away from our control, away from our oversight these vital, critical elements of our institution, is as meaningless as the notion of your white, puffy, harmless balls of cotton in the sky. The clouds that you like to think of.

When I hear "clouds," I think about thunder clouds. I think about menacing, dark, grey terror that knocks out servers. As they've done twice this year to Amazon. Mr. Chairman.

[applause]

Brad: Mr. Waggener, would you like to offer a one minute response?

Shel: One minute is more than enough time for a response to this particular line of argument, in that the proposal is simply that we are safer and better maintaining all of our resources internally. To do so ignores the fact that the vast majority of security breaches occur internally. As the Electronic Frontier Foundation has identified and the Cloud Security Alliance is documenting... There have been over 700 breaches that have occurred, simply because of internal negligence or internal failure to maintain security protocols... That has exposed 10 million records in the education community alone. Suggesting that, somehow, having a cloud provider would be less secure than our own community ignores the facts.

Brad: Professor Cate, one minute response.

Fred: Thank you, very much. Your argument, in fact, based on data, works wonderfully. It is true. In 2005, in 2006, higher education institutions accounted for almost a third of all reported breaches. In recent years, however, in the modern age, higher education institutions account for less than five percent, to be replaced by IT providers, which now account for the largest single sector of security breaches. Instead of taking what we have learned over the past decade, the success that we have achieved, and building on that, you want to take that information and give it to somebody else who's in the nascent stages of learning how to protect data in a cloud.

You may know, Steven Wozniak said earlier this month, "With the cloud, you don't own anything. You already signed it away." The more we transfer everything into the web, into the cloud, the less we're going to have control over it, and the less security we're going to have.

Brad: Time. Our first question of the day will begin with Professor Cate. In spring, one of the largest cloud providers in the world, Facebook, had its IPO. You wrote at that time that Facebook is monetizing a little piece of each of us. Since that time, the users and the growth Facebook has only gone north, while the valuation of companies who believe that they had struck the motherload of all of its great personal information, has only gone south, cutting the value of the company almost in half.

Professor Cate, hasn't the market and human behavior spoken this is OK?

Fred: I think in many ways the market has spoken. And frankly, I for one would not follow the crowd with our security. So the crowd, 900 million people in the world, has decided they will put

their most sensitive information on Facebook. They're idiots. It's a bad place to put data. [applause]

Fred: The fact that Facebook can make money off of our cupidity is not surprising at all. Whether Facebook creates a model on which we should follow, in terms of protecting our own institutional data is, of course, a completely different question. I think anyone who has seen the breaches that Facebook has suffered, has seen the changes of terms of service, has seen the difficulty that individuals have getting control of their own data in the Facebook environment would argue that Facebook is the perfect example for why we would not want our data in the cloud.

Brad: Mr. Waggener, hasn't the market said that this is all OK?

Shel: It's clear that with Professor Cate's perspective that 900 million people are idiots for sharing whether Fluffy managed to catch the ball or not as their most sensitive data in Facebook, or what they had for lunch is something that we need to protect with all investment, I think, negates the value of engaging 900 million people. The Arab Spring simply doesn't occur without connecting people in new ways. Which is more valuable, the freedom of an entire population or protecting pictures of Fluffy? [applause]

Brad: Next question, to Mr. Waggener. If humans are the weakest link in any security apparatus, how are we better by concentrating all of our data and all of our exposure where the inevitable possibility of a human error would expose us all, not just one campus or one department?

Shel: It's a fair question. Many of the failing that occur are the result of human error. Whether they are professional IT staff, individual consumers, or, in fact, entire companies of people dedicated to these services. I would argue that the greatest failing, thus far, has been the security research community that has not yet updated and adapted their practices, to accommodate for the kind of scale that we're dealing with now, in the cloud. It is not that individual humans make mistakes. It is that a community anticipates that they can code around that problem. We need to continue to find ways to improve the education and the engagement of every individual with what their responsibilities are in computing. That has nothing to do with the cloud. That has everything to do with the training aspects of people's preparations for using computing.

You would no more give keys to a three year old, to a sports car, then you would send somebody out to begin putting all of their data into the cloud without training. Yet, in fact, we do that today in our own computers, at home. People perceive that, by putting a password in, they're secure. Then they proceed to use that same password in every system that they connect to.

That's not a failure of a system.

That's a failure of an educational process.

Brad: Professor Cate.

Fred: I'm a little concerned about how to respond to Fluffy. The problem that we face here is one, as he puts it, of adaptation. And I, for once, agree with him. The security research

community has not adapted. We are not yet in a position where security is at a point that we want to concentrate all of our assets in one location and draw a target around it. The Gardner Group has what it describes as a hype cycle for new technologies. It starts with a technology trigger. We've certainly passed that with cloud computing. It then heads into the peak of inflated expectations, and I think that's where we are, before it crashes into what Gardner calls the trough of disillusionment. Gardner believes that we are just beginning to go over the edge, into the trough of disillusionment, with cloud computing.

This is a wonderful time to invest in a new technology. Just as it's heading down is the time you want to commit your most valuable assets to this unproven and untried system.

Shel: I find myself loathe to put my name associated with the Gardner hype cycle in any way, but recognizing that following the trough of disillusionment, which comes from individuals with polar positions, unwilling to accept trends and direction, it is followed by the slope of enlightenment. Which is the result of people learning and experimenting and advancing new solutions. You would have us stay, not in the Trough of Disillusionment, but in the antiquated position of the server hugger world.

Brad: I would have you not experiment with my data. [applause]

Brad: The next question goes to Professor Cate. Professor Cate, one of the centers that your run is the Center for Applied Cyber-security Research. And another one called the Center for Law, Ethics and Research on Health Information. You are a very strong advocate of security and policy and getting policy and the rules right. If the policy and the rules can't protect us, is your work meaningless?

Fred: Yes, it could easily be that case.

Shel: For once, we are in complete agreement. [laughter]

Fred: More to the point, we are exactly at the point where we don't have rational policies. We don't have standards around cloud computing. Everyone in the security world agrees that the three greatest vulnerabilities in any system of protecting data are the humans, the supply chain and, ultimately, the government. Because the government, depending upon where the data are located, get access to everything. We've not done a good job with any of the three of those. But we're not going to do better by punting them to be farther away from us. We at least know our own humans. We have no idea, when we put our data in the cloud, who their humans are. We have no idea even where they are located.

Similarly with the supply chain, we can verify our own supply chain. We can conduct audits. We can rely on the experience of others. But with a supply chain where we don't even know who the suppliers are... And remember, in almost all of the significant outages we have seen from cloud service providers, they have ultimately been blamed on either humans or a supply chain problem.

You may remember, one of the earliest examples we had of this, involving hospital records that were being processed by a company in San Francisco. I believe that's the state that you're from, in California. Sent that, of course, to a company in India, which sub-contracted it to a company in Bangladesh, which then neglected to pay its employees.

Whereupon they posted the records online. No amount of contracting, no amount of policy is going to protect us against that risk. And, of course, the final is the government. Anywhere the data are located, the government gets access to them. So when we store our information in a cloud, without knowing where that cloud is, in what jurisdiction, we might as well just be posting it on the web with a, "Come and get it," sign.

[applause]

Brad: Mr. Waggener.

Shel: Indiana University's esteemed medical program, hospitals and the medical school, have been using transcription services for years, in providing transcription of materials to third parties to transcribe into text. Because those were historically sent via cassette tapes to third parties you're suggesting that that is a far more secure way than what they do today, which is to digitize it and then send it over the network. It seems to me the problem existed long before the cloud became the more efficient and effective way to distribute information and simply resulted in cost-savings.

Whether you have a good partner or not, has nothing to do with the cloud. It has everything to do with your ability to understand the risks involved in any engagement and to ensure that you have the proper oversight in place.

Brad: Gentlemen, I'll do my own follow up with you on that one. There are risks in many things we do. I carry a piece of plastic in my wallet. I fly just about anywhere in the world. I procure services and readily give that number to someone who pays my hotel bill, whatever. There is a certain amount of fraud that goes on around credit cards and debit cards, but haven't we really worked that out? Over time, the market was self correcting. The risk was there. The behavior sorted itself out. The policy, the security standards. Won't this situation really fix itself? Professor Cate?

Fred: The answer is, no. The market didn't fix that situation, either. Congress fixed that situation. It passed a law saying no individual could be liable for more than $50 for the fraudulent use of a credit card. It passed that law 40 years ago and 40 years of experience when all of the financial responsibility was shifted to the card issuer has taught card issuers to be really careful. They do a wonderful job. We have no liability shifting now in cloud computing. Cloud computing. A cloud computing company loses your data, a cloud computing company is hacked, a cloud computing company goes down. Congress has said nothing about what happens there. That's exactly the point about this being in the infancy. There will come a time when we will have well established standards of behavior and it may then be that certain data can appropriately be put in the cloud.

But think about the experience of Mat Honan and Wired. Remember, his most sensitive data, his pictures of his child's first year on this Earth were stolen and deleted because two well respected companies, Apple and Amazon, each were so busy to accommodate their distant customers that they allowed any stranger to come in and hack the account and delete the data.

What saved his data, what brought back two thirds of those pictures, the fact he had a local backup in his home. The cloud would have killed him.

[applause]

Brad: Mr. Waggener. Fred, Fred, Fred. Do you still travel with a wad of cash and traveler's checks, by chance?

Fred: I use the credit cards that are protected by law.

Brad: You probably use some fat cat academic expense account is really what you do. I think the real issue here is that the credit card laws were passed not before the credit card industry existed. Not before BankAmericard was created. But, in fact, once it reached a certain scale that the community was able to voice it's needs and laws were passed. You're suggesting that the government step in and prevent evolution and advancement of cloud computing until we get it perfect. I would think, as a technologist, even you would recognize that there is no such thing as perfect. But rather, continued enhancement and improvement. We have seen laws passed in 50 states now, providing data protection.

Each state has taken a slightly different approach. As a result, the federal government is now getting involved and looking to enhance data protection standards on a national basis. You saw many states exempt commerce from taxation when the cloud first began, and now you're seeing taxation come into the fold with cloud providers.

That's because we have learned, we have experienced how to advance those technologies and they've now reached the point where billions of transactions are handled safely with your data in the cloud. The fact that a breech occurs is not the result of the cloud as a community failing, but rather the result of individual failings which occur whether you're in the cloud or not.

Fred: The difficulty here, Fluffy, is that you're wrong on a matter of law. To begin with, the credit card protection was created over the objections of industry which said, "We don't need any standards. We'll take care of it." But it was consumers who said, "We need protection," and Congress acted to protect them. Secondly, the 50 states that you refer to as having enacted security standards may be some place, but they're not in this country. In this country 47 states have enacted breech notification laws. Get this. This is what he called good security. We'll tell you after we've lost your data. That's a good standard. To date, only one state has enacted a state security standard law, and that's the state of Massachusetts. So if you want to put your data in the cloud, I'd go to Massachusetts.

Because at least there, there is some legally required minimum standard for security of data.

Shel: The data security laws you're referring to were designed for notification of internal breaches from internal companies, not for the cloud. They were not customized for the cloud. They, in fact, pre-date much of the use of the cloud. They're the result of internal breaches and internal failings. They are designed for medical communities that have your medical data. Are you suggesting that those entities, your hospital, would be better off without your data? So that, when you have an emergency and you go to an emergency room, they're able to say, "Could you please produce your parchment that has all your records on it and we'll be happy to treat you after we have reviewed all materials."

Or do you want your provider to actually be able to help you in those cases. I think no response is necessary. We know where you'd rather be.

Brad: Next question, to Mr. Wagner. During the year of 2008 and 2009, we saw the economy of the United States essentially melt down and part of a global financial crisis. Much of that crisis in the United States was in the housing market and other big banks that have become too big to fail. In the aftermath of assessing that horrendous massive damage to the U.S. economy, we see almost no one was responsible, that each bank was dependent on another bank. They were all individually following the rules and such.

So if we fast-forward to cloud computing today, here at Indiana University we have students who want services. As the CIO, I sign the contract with a firm you're familiar with called Internet2. Internet2 signs a contract with a firm called Box. Box doesn't run its own data centers. It uses a network contracted from someone and a data center provided by someone else.

Is the cloud not just the next financial house of cards?

Shel: I think there's a very real possibility that if we don't as a community take responsibility for ensuring that we have good security protections in place, not just with the primary provider, but in fact with the data. In that context, what are your encryption standards? Data is provided to your community via Box. The data is then encrypted, so that regardless of the breach or failure that may occur further on, you maintain controls around how your data is stored and protected.

That becomes a very important part of an overall ecosystem of protection, so that you're not relying on any one player in the ecosystem. You're relying on everybody to do their part. And, most importantly, you're relying on yourself to do yours.

Brad: Professor Cate.

Fred: I think you've put it well. I think it is a house of cards. One question we might ask is, "What happens when it comes crumbling down?" Which it will. So we have a little experience with this. One of the earliest consumer bankruptcies involving a data mining company was the company Toy Smart, which held data on children who had purchased toys online. Toy Smart was promising, by law, that it would never sell the data. Until it went bankrupt. Then the bankruptcy court said, "You only have one asset. That's data." Just like a cloud computing provider. Just like all of the service providers you talked about. If any chain in that link fails, the whole chain fails. But, worse than that, the asset that they all have in common is our data. Our data, which, at that point, is marketable. It has value. It can be sold to settle the debts of the bankrupt.

Brad: A response, Mr. Waggener.

Shel: I'm just trying to imagine what you purchased on Toy Smart.

Brad: A Winnie the Pooh watch, I do know that. [laughter]

Shel: Somehow I'm not surprised. I do think that protecting not just your personal data, but your overall digital persona, is something that is going to be an increasing challenge. For years, we have had courses for new freshmen coming in, to educate them about the danger of alcohol, engaging them in appropriate code of conduct. We now see the need to engage with them and

train them on digital persona and digital life. What does it mean to put your information with someone other than a trusted partner who you have physical presence with? Living in the digital world is a modern standard. Our new students coming in couldn't show you or tell you what a mimeograph machine was if you asked them, in spite of Professor Cate's classroom, which I'm sure has several available. The reality is, those students need this training and that education. They need to understand that once published digitally, likely never forgotten.

That is true of information you provide to your bank. It is true of information you provide to your DMV, to your government. It is true in many contexts. The assumption that you can simply not provide data to anyone and be a thriving member of society today is false on its face.

Brad: Next question to Professor Cate. I noticed that Mr. Waggener was carrying a digital device and knowing you personally, I know that you carry a digital device as well. As a matter of fact, Professor Cate, I recall the very first iPhone coming out, or in its first year, and you being someone who said, "This is my computer." You were amazed at its capabilities and started using it almost incessantly, for much of your work and such. The iPhone is really not that impressive, short of cloud services. Is there an inconsistency in your thought, in your action?

Fred: I think there's judgment in my thought or action. Which is, the way I treat my own data may be different than the way I expect you, as the custodian of the university's data, to treat those data. So, for example, for playing Tetris, the iPhone is fabulous. It is, perhaps, the best screen ever invented for that game. It also makes watching movies terrific. Even a small movie, you can really enjoy and, of course, on an airplane that's as about as far away as you can get with your screen.

But for putting your most sensitive data on, your tax returns, your banking, and so forth. You then have to use a different standard of judgment. That standard of judgment does not ultimately depend as much on the iPhone as it does with the partner on the other end of the transaction which you then make rational judgments about their dependability.

The problem we have seen with the iPhone is where Apple itself has failed to live up to its commitments. For example, we discovered a majority of apps were collecting data even though they weren't permitted to collect data. You could say that's a classic case of an early adoption problem, but at least it was a problem with the data that individuals chose to put there as opposed to having somebody else make the choice for them about data that are potentially far more valuable about the students, the applicants, the alums, the staff, and the faculty of the university.

Brad: Mr. Waggener.

Shel: I think it's fabulous that Professor Cate no longer pulls around the K-Pro machine behind him, or has to have a Commodore 64 taped to his arm. Because really, they're not very comfortable to carry around. The fact of the matter is, these are windows, not just into corporate data or personal data, they're windows into the world. You have access to information and resources that you simply would not have access to elsewhere. The vast majority of that isn't about protected, proprietary or custom data. It's about sharing information. So when you go to do that in a portable device, you have to know how to protect what is important. With that, I do agree with Professor Cate that you must have those standards in place.

For not just the company, but for yourself. And what security program have you installed on your iPhone, sir? You're assuming that it is secure because you are relying on one provider, Apple, to provide that security. I, however, have chosen to use an open standard device, installed open standard security protocols on this, and protect my data in multiple layers.

So aren't we really talking about a situation where your lack of knowledge, your lack of experience as a security professional, is really the risk here. Not the device itself.

Fred: I think we're talking about a situation in which the data I'm putting on there are simply less valuable and less vulnerable data. Judgment is what it's all about.

Shel: I don't know, my Tetris score is pretty damn important.

Brad: Next year's debate will be the rumble between the Android and iOS 6. A question from the audience, and I'll ask you each to be somewhat brief but specific. Could you enumerate what you personally put in the cloud? Mr. Waggener.

Shel: Well, I, like 40 percent of all Americans now, file my taxes electronically. We talk about who do we trust and who don't we trust. I probably trust the U.S. government less than most, but in fact, find the ability to have my electronic financial records transmitted to the government so that I can have my refund transmitted back to me faster, to be a real benefit. I also put much of my content into a three two one program. I have three places I keep all my data. Yes, I have data in iCloud and yes, I also have it in Amazon, and yes, I also have it at Google. But I have all my most sensitive data protected, also, with an on frame solution, in my home. As well as mirrored to a third location, so that I, at all times, have three copies on three different types of media of any of my data.

Is that an expense that most Americans will go through? No. But as the cost drops and the knowledge around how to protect it improves, I think you'll see many do just that.

Brad: So let's get specific. Mr. Waggener, do you use LinkedIn?

Shel: I do.

Brad: Do you use Facebook?

Shel: I do not.

Brad: Do you use cloud storage?

Shel: I use Box.

Brad: Is there anything that you're not comfortable using on the cloud, that you would not trust?

Shel: I don't provide my personal information to any cloud provider that asks for PII, personally identify viable information. I actually exclude those answers. I create my own security questions in all cases, rather than using the default security questions that are provided. And I use the same credit card, that has the highest level of protections, for my enrollments online. Such that I can monitor those transactions much faster than...

Brad: One more question, before we go to Professor Cate for his list. You hit a website, it asks and says... Let's say you hit Flickr, and you want to log in with your Google ID, which is allowed, and it asks you the question, "Will you allow Yahoo and Google to link your identities?" Yes or no?

Shel: No.

Brad: Professor Cate, your list.

Fred: I'm glad that Shel doesn't put his PII in the cloud, he just thinks you should put the rest of our PII in the cloud instead. I don't put any sensitive student information; I don't put anything regulated by FIRPA in the cloud. Because I don't think we can verify compliance with that. The types of less important information, which I do connect to through and iPhone or an iPad, I back-up entirely locally. On the assumption that they will almost certainly be compromised in the cloud and I'm going to want a pristine back-up copy to restore from. No, I don't use Facebook. No, I don't use Twitter. I don't think I use any of those things that you mentioned. I probably don't even know what some of them are. My own view, as it was, actually, with the iPhone...

Your recollection was slightly incorrect. I did not get the iPhone 1, because I wanted to wait for the iPhone next generation, to first let them fix the first round of certain problems.

That is very much where we are with cloud computing today. The notion of taking a huge collection of data and putting it some place far removed from us, where we have no direct control over it, may one day, in some future generation, or after enough drinks, make sense. It just doesn't yet.

Shel: So I'm sure 146 characters is too much for an academic like yourself to be able to master, but things like Twitter are not about personally identifiable information. They are about connecting things. So it would seem appropriate that when you're selecting services to use, you select them based on the appropriate use paradigm for those. I have a Facebook account. I created it the week that Facebook approached Berkley about joining Facebook, when it was first released and developed, long before it had millions of users. Not because I was going to use Facebook. Because I was exploring and deciding what the value of such a tool was for myself and my community.

I think you'll see that, in many cases, these services plan on advancing and growing far beyond where they are today. You should never count on that to be the case. You need to make sure that you're taking an appropriate precaution. The appropriate precaution is not to sit on the sidelines, 10 years after Salesforce.com began running production enterprise applications in the cloud.

It's not to sit back after there are 900 million accounts at Facebook. Not to sit back after there are hundreds of millions of Hotmail accounts and Gmail accounts... And say, "I'll wait until I'm entirely certain everything is perfect." That day is never going to arrive.

Brad: From our audience, Perhaps this whole debate is focusing on the wrong topic. Human behavior evolves. For example, the courting rituals and the period of dress that we saw from Brian and Daphne. A gentleman would make a reservation to come call on a lady before

anything took the next step in the courting ritual. Not so much today. Human behavior evolves. This obsession with privacy, is it perhaps not just a 20th century notion, Professor Cate? That you're really thinking about solving a problem that this generation doesn't care about.

Fred: That's just not true. We know well that this generation cares about privacy. They don't care about it the way that we do. They don't think about it as the same thing. So, for example, your reference to the courting ritual. Today, sharing a password is considered a sign of trust. So, in the way that we might have exchanged rings or exchanged promises 100 years ago, today, exchanging a password is an indicator of trust. It's a bond.

Brad: You just sent Tom Davis, our security officer, into orbit. [laughter]

Fred: It's a bad indicator of trust, but it is a common one. And it is easily revoked, as are most relationships. But having said... Whenever people say, "This generation doesn't care about privacy," you can just look at the reaction to specific things that challenged their view of privacy. I used to deal with this issue in class where students would say, "I'm not that worried about privacy." I would lug in a collection of their application files and say, "I'm going to read you each other's application essay and let's see if you've changed since then." I don't get five words into it before they're like, "Stop!" They suddenly think of that as privacy. They also have a much more subtle notion of privacy, which cares about circles of trust.

You and I might share something, but we don't want him to know about it, for obvious reasons. This concept of privacy is one that, again, cloud computing and services like Facebook, have given the illusion, but not the reality, of.

Brad: Mr. Waggener, privacy.

Shel: I think it's fair to assume that privacy standards will continue to evolve as appropriate dress, appropriate decorum in any professional setting has evolved over time. It doesn't mean it's worse today. It means it's different. For those desperate individuals clinging to the past and wishing to maintain a set of standards that are no longer valid in today's society professor. I believe that it is possible to even help those folks move forward by recognizing that what is rude in the real world is just as rude online. What is appropriate in the real world can be appropriate online. The difference is scale. You may make an off color comment or an off color joke to close friends and associates that you would never make to a room of a hundred or a thousand or a ten thousand or ten million. I think it's reasonably certain that 47 percent of the US was not overly thrilled with an off color comment made by one of the candidates recently because there was never an expectation that that would go to 100 million people.

But does that mean that it's the cloud's fault that those words were uttered? Is it the cloud's fault that a complete idiot would make a video that would enrage a billion people? No, those are standards of free speech. Those are standards of decorum which transcend the cloud, and calling an individual an idiot is something that we all still have the right to do. You just need to recognize that just as this is being streamed and will be viewed many times over, I would never make such a statement about my esteemed colleague, whether I believed it was true or not.

[audience cheers]

Brad: Gentlemen, in a final question, we've shown a tremendous ability to adapt to change over time. That is, human society. As technology marches on, as human behavior adapts and marches on, as the economics change and march on, we tend to get this right over some amount of time. So isn't the real debate here only about the pace of these problems being solved and the pace of how much we engage? So first, to you, Professor Cate. Give me some advice as an IT leader and the leaders in this community. Give us some advice. What is the right pace for cloud?

Fred: Let me first say I don't agree that it is just a question of pace. We have seen technology move down many what you might call dead ends. We've seen eight track tape. We've seen cassette tape. We've seen digital audio tape. How many of you invested in that? We've seen the evolution of technologies that are then replaced by something else, and there's no indication that this is not simply a fad that, like those, will whether it happens quickly or slowly, will pass. The question is rather how much do you want to invest in an unproven technology in an unproven system, when by putting critical data into it, you may make it that much harder not only to secure it but to get those data out when you need them reliably, 24/7, 365 days a year.

So what I would suggest is not to eschew cloud. That's why the campaign slogan is not cloud never. Also because Daphne thought it didn't rhyme. But also because it's simply cloud not yet.

Not until we have better experience with it before we put institutional data in it. Not before binding legal standards are developed that tell you where liability is going to be found when things go wrong, which they inevitably will. Not before there are clear security standards on what good background checks mean, on what appropriate oversight, on what auditing looks like in the cloud.

What you don't want to be is the test case that demonstrates that. And therefore the right pace is not to say never, it's to say not yet.

Brad: Mr. Waggener, as the spiritual leader of the Cloud Now party and the chief architect among colleges and universities, what is the right pace for cloud?

Shel: I can appreciate the bitter feelings that Professor Cates has over his Betamax collection today. But believing that the best approach is to sit on the sidelines, and to allow any technology evolution to occur -- without your involvement, without your engagement, without your input, without your insights, and just as significantly, without our communal insights, without our collaboration across our community and higher education, where we are the standard bearers when it comes to discovery and when it comes to research into new directions -- thinking that the best approach is to wait until all the problems are solved simply goes against the core ethos of the academy. I believe that the right pace of change is recognizing that the pace of change is accelerating whether we want it to or not. I'm sure living in Mayberry was a wonderful thing; we'd all like to go back there. But remember, Mayberry never actually existed. It was imaginary, and it was proposed as an idyllic scenario for all of us to escape to. I'd rather not escape anywhere; I'd rather be part of that change. And I think being involved in the cloud today gives us the opportunity to influence it rather than to sit by and wait, and wait, and wait, and then eventually recognize that no one else has a Betamax to play your tapes on.

[applause]

Brad: And with that we will draw our debate to a close. I offer a couple of footnotes: First off, Bloomington is very close to Mayberry and we do enjoy that. And I do recall Johnny Cash sounded quite good on eight-track, for your memory as well. We are grateful to our sponsor of Smithville for helping to put on this debate. And let's give each of our party leaders a great hand for their debate. [applause]

Shel: Unity. [music]

Brian: So Brad said that we needed wardrobe help. We think we fixed it.

Daphne: He said we were a little confused, and he was right. Everyone knows I wear the top hat.

Brian: So how was the debate? Who won? [shouts from audience]

Brian: Well we're about to let you go to break, we'll just take a second. We want to give a special thanks to the diamond sponsor this year, which is Matrix Integration. And be sure to visit the booth while you're out there and also get some food. We paid for it.

Daphne: Come back from break promptly at 10:30. There's going to be a special start to Brad's keynote this year that we're pretty sure that you guys don't want to miss, and we say that in all seriousness. So thank you. Hope you enjoyed the debate.

Brian: All right. Thanks. Bye, bye. [applause]

Man 1: Hey, I'm going to tell you all the same thing Sonny Lance Lemon has been trying to tell you for years. Be careful how you vote. [music]

Transcription by CastingWords