NATIONAL PRESS CLUB LUNCHEON WITH VINT CERF

SUBJECT: VINT CERF WILL DISCUSS THE INTERNET OF THINGS AND THE FUTURE OF THE WEB

MODERATOR: JOHN HUGHES, PRESIDENT OF THE NATIONAL PRESS CLUB

LOCATION: THE NPC BALLROOM, WASHINGTON, D.C.

TIME: 12:30 P.M. EDT

DATE: MONDAY, MAY 4, 2015

(C) COPYRIGHT 2008, NATIONAL PRESS CLUB, 529 14TH STREET, WASHINGTON, DC - 20045, USA. ALL RIGHTS RESERVED. ANY REPRODUCTION, REDISTRIBUTION OR RETRANSMISSION IS EXPRESSLY PROHIBITED.

UNAUTHORIZED REPRODUCTION, REDISTRIBUTION OR RETRANSMISSION CONSTITUTES A MISAPPROPRIATION UNDER APPLICABLE UNFAIR COMPETITION LAW, AND THE NATIONAL PRESS CLUB RESERVES THE RIGHT TO PURSUE ALL REMEDIES AVAILABLE TO IT IN RESPECT TO SUCH MISAPPROPRIATION.

FOR INFORMATION ON BECOMING A MEMBER OF THE NATIONAL PRESS CLUB, PLEASE CALL 202-662-7505.

JOHN HUGHES: (Sounds gavel.) Good afternoon, and welcome. My name is John Hughes. I'm an editor for Bloomberg First Word, that's our breaking news desk here in Washington, and I am the President of the National Press Club. We are the world's leading organization for journalists. We are committed to our profession's future through programs just like this, and we fight for a free press worldwide. For more information about the Club, visit our website Press.org. And to donate to programs offered through our Club's Journalism Institute, visit Press.org/institute.

On behalf of our members worldwide, I want to welcome people in our audience to today's Newsmaker luncheon. I'd also like to welcome our C-SPAN and Public Radio audiences. You can follow the action on Twitter using the hashtag NPClunch. Remember, the public attends our lunches. Applause is not evidence of a lack of journalistic objectivity. After our guest's speech, we'll have a question and answer period. I will ask as many questions as time permits.

Our head table includes guests of our speaker and working journalists who are Club members. Let me introduce them to you now. I would ask each person to stand briefly as names are announced. From the audience's right, Pender McCarter, retired Public Relations Director for IEEE. Jackie Kasel[?], former Presidential Innovation Fellow at the White House, FEMA and GSA. Biol Yarnoff[?], Vice-President of Business Development at the Diplomatic Courier. Pam Harbor, technology freelancer and Chair of the National Press Club's Freelance Committee. Jonathan Fisher, Senior Editor at Slate. Susan Molinari, Vice-President of Public Policy and Government Relations at

Google and a guest of our speaker. Allison Fitzgerald, Managing Editor at the Center for Public Integrity and a member of the National Press Club Board of Governors.

Skipping over our speaker for a moment, Laurie Russo, Managing Director at Stanton Communications and the Speakers Committee member who organized today's Lunch. Thank you Laurie. Hayley Tsukayama, Technology Reporter for the Washington Post. Tom Risen, Technology Reporter for US News and World Report. Wayne Rash, Washington Bureau Chief for e-Week. Joshua Higgins, Technology Reporter for Inside Washington Publishers.

[applause]

So a little more than 40 years ago, the first international conference on computer communication gathered in the basement of the Washington Hilton. Attendees witnessed the demonstration of new technology that enabled advanced applications to run between computers here in Washington and others around the country. OptiNet, a network created by the Advanced Research Projects Agency was the earliest version of the internet.

One of those involved in the demonstration that day is today's speaker. Since then, in 1972, Vint Cerf has developed and advanced the architecture and utility of the internet, ushered the continued spread of the web, and become one of the most widely respected authorities on internet policy and governance. Many call him a "Father of the Internet."

Since 2005, Dr. Cerf has served as the Chief Internet Evangelist for Google. He says he took that moniker because they wouldn't approve the title of "Archduke." Dr. Cerf is obviously well versed on the value and capabilities of the internet. Recently, he voiced concern that the 21st century could become an information black hole unless we find ways to preserve photos, documents and other digital content, which is hard, because we don't know how computers of the future will function. His solution for now, if you want to make sure that some important information survives for posterity, print it out.

[laughter]

Dr. Cerf's current project is the interplanetary internet, which he is working on with NASA's Jet Propulsion Laboratory. It is exactly what it sounds like, a computer network for planet to planet communication. His list of awards and commendations is, as you can imagine, quite lengthy. If you want to learn more about them, you'll just have to look them up on the internet. [laughter]

__: Google it. [laughter]

JOHN HUGHES: Please give a warm National Press Club welcome to Google's Chief Internet Evangelist, Vint Cerf.

[applause]

VINT CERF: Well first of all, thank you very much. This is theorem number 2008, which reads, “If you feed them, they’ll come.” And here you are. And I'm here too. So it’s my favorite theorem, and I'm glad we proved it again. Second, I'm not going to use any presentation charts or anything. My motto is, “Power corrupts and PowerPoint corrupts, absolutely.” So you’ll have to just listen to Vint instead.

I did want to tell you a little anecdote which I think is relevant to especially this population. I worked on something called MCI Mail way back in the 1980s. We turned it on, on September 27th, 1983. And among the first people to sign up for this electronic mail service were reporters, one of whom was William F. Buckley. And I maintained a one-way correspondence with Bill over time before he passed away. And I remember that I had come and gone to MCI, built MCI Mail, left to join Bob Kahn at CNRI and rejoined MCI to help them get into the internet business.

And around 2003, it was very clear that charging people for email wasn’t exactly a great business model anymore. So we shut down the MCI Mail Service. And I got a whole bunch of angry emails from reporters, who said, “I've had my MCI Mail address since 1983. How can you do this?” But the honest answer is that it was time for that service to go.

So I have two themes that I would like to address this afternoon. The first one has to do with technology. And I will drop into geek a bit, but I apologize, but it’s the only way to be precise. And then I want to talk a little bit about policies. Now, I have eight points or so on the tech side and four or five points on the policy side. So let me start on the technology side.

I'm really proud of the fact that the internet continues to evolve. This is not a design which was fixed in time 40 years ago, but rather it’s one which has adapted to new technologies and swept in new communications capabilities. It’s become an important element of the smart phone, both the internet and the smart phones and the world wide web are all mutually reinforcing in many, many ways.

So one of the things that Bob and I didn’t quite get right was the amount of numerical address space that's needed in the internet. When we designed it 40 years ago, we did some calculations and estimated that 4.3 billion terminations ought to be enough for an experiment. And so the version of the network that most of you are using is called IP version 4, or PCP IP version 4, which was designed back around that time.

Well, we got it wrong. We ran out of the IP version 4 experimental address space around 2011. The CEO of ARIN, the Americas Registry for Internet Numbers is right over there, John Kern. You can wave at them. So if you need IP addresses, he’s the guy to talk to about that. I am proud to serve as Chairman of the Board of ARIN.

But we need IP v. 6 now, which has 128 bits of address space. I’ll do the math. It’s 3.4 times 10 to the 38th addresses. This is a number only that Congress can appreciate. [laughter] But it is absolutely vital that we get all of the ISPs to turn IP v. 6 on. The software is in your laptops and desktops and mobiles. It’s in the routers. But the internet service providers need to turn that on in parallel with the IP version 4 service, which many of you are using today.

So you can do me two favors. One, as individuals, talk to your ISPs and demand an answer, “When am I going to get IP v. 6 addresses? I want dates and times.” And second, as reporters, will you kindly do the same thing, but do so with the megaphone that is afforded to you by the Fourth Estate.

Now, why do I care about having lots more IP addresses? Well one answer is, the next wave of stuff is the internet of things. You all know that. But this is real. Every appliance that you can possibly imagine is shifting from electromechanical controls to programmable controls. And once you put a computer inside of anything, there is an opportunity to put it on the net. Now, there are good things and bad things about that. The good thing about the internet is, everything is connected. The bad thing about the internet is everything is connected.

So we really need the address space in order to accommodate this explosion of devices. Sysco says that there may be 50 billion devices by 2020. And they may not be as crazy as it sounds, because every light bulb could potentially have its own IP address. Some of them already do, like the light bulbs that are made by Philips, called HUE, not HUGH. You can control the color and the light intensity from your mobile. And to do that, you need an internet address.

So we need to get IP v. 6 implemented. That’s the first technology point. The second one is even more obscure. The label is buffer bloat. And you might think, “Okay, so what is this?” When you're watching streaming videos, have you ever noticed that sometimes they get really jerky, and things slow down, and the delays are going up, and you sit there, waiting for things to reload?

Well it turns out that it is not true that having more buffer memory space is always a good thing. Let me explain. You have a router at home, typically. Maybe it’s supplied by cable or Telco company. Or maybe you bought one and installed it, or you hired a geek to do that.

And so this thing has memory in it. And imagine, for a moment, that you're running a local network at home, and it’s running at maybe 100 megabits a second, or maybe 10 megabits, or maybe even a gigabit per second. But the connection that you have out to the rest of the world is not running that fast, unless you happen to be on one of the Google fiber networks, in which case you're getting a gigabit per second. But most of them don’t quite get to that speed.

So what happens? The program that you have running inside the house is pushing data like crazy into this buffer, which is filling up, and emptying slowly, because the data rate on the other end is slower than the rate at which you're pumping it in, which means that there is increasing amounts of delay, from the standpoint of this sender over here, waiting to hear acknowledgements coming back from the other end.

At some point, the program inside your house is saying, “Oh my God, they didn’t get what I said. I’d better send it again.” And so you keep re-transmitting. And pretty soon you create a highly congested condition. So it’s counterintuitive. But what you have to do is to design the system so that it doesn't put too much buffer space in the path. It should put only enough to deal with the differential between the high speed and low speed side. Of course this also works in the other direction.

So there is-- here is the code word for you. The letters that you want to refer to are called CODEL-FQ. CODEL-FQ. And that is the kind of thing, that’s the technology that you want in your routers. So, while you're pounding on the table for IP v. 6, you could say, “And also, by the way, I want CODEL-FQ in my router. And I want a pony.” [laughter]

Okay. next point. All of you are familiar with the fact that we’re really bad at picking passwords. And some of us still use “PASSWORD” for our passwords, because that’s easy to remember. But everybody else knows that, so that’s not a good thing. So, you try to-- You're told, “Please make up complicated passwords with punctuation and other stuff. And keep changing them all the time.” And you can never remember them, so you make a list, and you stick it on your computer. Or you put it in your wallet.

Okay. So, at Google, you will remember, and some of you reported that we were attacked in 2010 and penetrated. And so we decided we needed to do something about that. So, in addition to user name and password, which we still ask people to change on a regular basis, we also have a piece of hardware. It is called a GNUBBY-- and don’t ask me why. I have no idea. This little gadget is a two-factor authentication device. Essentially, it generates a random one-time password using the cryptographic algorithm.

So when I log into my Google accounts-- and you could do this too if you were using Gmail-- When you log into the account, if you're asking for two-factor authentication, it will do one of several things. If you have this little device, you just tickle it, because the light came on, and it sends the data back and forth. Or, it sends you a random number to your mobile. Or, you have an algorithm running in the mobile that generates the random number for you.

All of those cases imply you had to have this other thing, your mobile or the little GNUBBY device, or a message coming from Google giving you the latest one-time password, in addition to knowing your user name and password. So that’s why it’s two-factor authentication. It means if somebody got your user name and password for any reason at all, they can't-- they can't get in, because they don’t have the second factor. We would like to encourage everyone to adopt that practice, because that will make the network safer for you and for me.

Fourth point. Security is, and safety and privacy are really important in the net. And one way to achieve that, in part, is to use what's called HTTPS, HyperText Transport Protocols, what Tim Berners-Lee invented back in late 1989, and released that as part of the worldwide web, there is a secure version of this. It’s called HTTPS. And the purpose behind it is to encrypt the traffic between you, your laptop, desktop, mobile, tablet, and the server on the other end, Google in my case.

And so the idea here is that everyone should be making use of this cryptographic means of transmitting data back and forth. So, while you are using web-based applications, the information is kept in encrypted form and only decrypted when it reaches the other end. So this is called encryption for transmission.

Which leads me to the fifth point, which is that Google and others believe that all transmissions, regardless of whether it’s from your Edge device to our services or between our data centers or any other place, ought to be encrypted in order to protect confidentiality. And so we see crypto as a very, very important technology which should be incorporated into normal use on the net.

I know I don’t have very much time. So I won't tell you stories about how I worked with NSA way back in 1975 to design and build a secured internet. The only problem was that the details were classified at the time, and I couldn’t share it with my colleagues. So I felt schizophrenic for a long time. But now we have the technology available to make this a much more confidential environment.

We think, also, that it’s important to encrypt data once it lands in place. So your laptops should be encrypted. Your disc drives should be encrypted. Your mobiles should be encrypted. We will encrypt data that lands in our data centers as we move it back and forth between the data centers, we keep it encrypted, so that even if the data center were penetrated or you lost your laptop or your tablet, the information will be very hard for someone to extract. So crypto is important.

The seventh point is another geek thing, it’s called DNS SEC. Now you all know what the domain name system is, because you use domain names all the time. DNS SEC is a security extension. How do I do this in a couple of seconds? When you do a lookup of a domain name, you may not see that happening, but when you type www.google.com, your computer says, “Where the hell is that on the net? I need a number.” And it looks it up in the domain name system, which is a big distributed database.

What it gets back is an IP numerical address. So these two pieces of information, domain name and IP address, are very important. Now what happens if somebody can go in and change the numeric address associated with the domain name? You may think you're logging into BankofAmerica.com. But if somebody has hacked the system, you're off to some bad site, which is tracking your user name and password and everything else.

So the solution to this problem is to use something called a digital signature. Some of you have heard the term “public geek cryptography,” digital signatures arise out of that technology. We can digitally sign the binding between the domain name and the IP address. So, when you get that pair back from doing the query, you can check, “Did anybody change the binding? Has anybody altered the numerical part?” And by checking the digital signature, you can verify it has not been modified.

This protects against all kinds of spoofing kinds of attacks that would otherwise be of harm. So we think DNS SEC should be implemented. It is being implemented throughout the domain name system. But we need more and more implementation as it goes down into the hierarchy.

The eighth thing on the geek side-- you're going to love this-- it’s BCP 38. Okay, what the hell is that? This is Best Communications Practices Number 38. Basically, what this says is that, if you are operating a network, and you are going to accept traffic from people that will eventually be sent out to the rest of the internet, the first thing you should do is check to see whether the source internet address, the numerical internet traffic into the net that has fake source addresses. It’s possible to fake the source address by just stating, “This is coming from that place over there,” even though it’s coming from here.

We don’t want people to do that. So we think, again, the ISPs should be executing this BCP 38 thing. So you can tell that I have a very strong message, which I ask you to amplify, to tell the ISPs, time to get on the stick to improve the safety, security and confidentiality of the net.

Okay. Now, we’ll switch over to policy. And they told me they were going to tell me when this thing was going to die. It says I have19 minutes left?

JOHN HUGHES: No, it says it’s 19 after. So you’ve got--

VINT CERF: Three and a half seconds?

JOHN HUGHES: Seven minutes.

VINT CERF: Seven minutes, okay. Okay. So eight things in seven minutes. First of all, some of you, I hope, are reading about, and some of you may be writing about, this idea that NTIA, the National Telecommunications and Information Agency has to transfer whatever responsibilities it still retains to the internet corporation for assigned names and numbers. This is called the IANA Transition, the Internet Assigned Numbers Authority Transition, so that the multi-stakeholder bodies of the internet, all of us, become part of the operation of policy development for the internet, rather than having a specific agency of the U.S. government taking responsibility for that.

When the ICANN was created in 1998, that was the intent. There was supposed to be a two or three-year period, while everything settled down, and then NTIA-- then NTIA would then relinquish responsibility for any further direct interaction. Well, it’s been some years since 1998. It’s now time. And NTIA has proposed to do that. It’s asked the community to show how it would operate without the benefit of this NTIA oversight.

And so, although there is controversy over this, I am a strong believer that we should step-- the government should step away from this special responsibility or authority and return this to the community, which has created and operated the internet since its inception. So that's point number one.

Second, I can't imagine that you would disagree, that freedom of expression and access to information is absolutely fundamental to our Democratic societies. And we need to make sure that the internet continues to support that. I'd like to add one more freedom to this. And that's freedom from harm. We don't often speak about that. But, unless people feel that they are safe in using the internet, then they will not use it. And if they don't, then some companies' business models, including mine, may be very well be undermined. So it's very, very important, in addition to the freedom of expression and assembly and access to information that we do everything we can to protect people from harm, which is why I was talking about all those other geek things a little while ago.

Point number three has to do with non-discrimination. And in particular, none of the ISPs or the broadband providers should have anything at all to say about where the traffic comes from and where it's going. Everybody should have equal access to the net. You should have the ability to go anywhere you want to on the net, and in principle, do whatever it is you want to do. Of course, if it turns out to be illegal, that's a different problem. But none of the providers of access to this system should be telling you what you can and can't do. So that's a non-discrimination element. That's trilling up in the net neutrality orders that have come from the FCC.

Preserving user choice is fundamental, again, to the internet's utility. Similarly, the fourth item on the policy list, is equal access to performance features. I mean if you have the need for low latency because you're playing some kind of a videogame, or you need high bandwidth because you're streaming video, you should have access to that. There shouldn't be possible for the broadband provider to pick and choose who gets access to that and who doesn't. this should be openly available to everyone. I didn't say free. But what I said is everyone should have equal access to those capabilities.

And finally, I think it's very important that we encourage, not only here in the U.S. but everywhere around the world, the adoption of policies that would encourage the creation of more internet. Now, of course, I'd say that. But look. Here is my problem. At Google, my job is to get more internet built all around the world. And, in talking to Eric Schmidt the other day, he said, "You know, you can't retire." And I said, "Well, why not?" And he said, "Well, you're only half done. You have three billion people up. You have another four billion people to go."

So I could use some help in case any of you are interested. We really need to help countries recognize the importance of investment in internet infrastructure for the benefit of their citizens. And so that is my fifth and last point on policy. And, since I am clearly over time, I will stop there, Mr. Chairman, and turn the floor over to you to ask grilling questions.

Thank you.

[applause]

JOHN HUGHES: Thank you very much. The internet was created by the U.S. Defense Advanced Research Projects Agency, or DARPA. And now, it is global. Yet no one really owns the internet. Is it possible that a multi-stakeholder governance environment can actually work?

VINT CERF: Boy, that was a nice gimme. Thank you for that one. I appreciate it. First of all, he's right. DARPA did sponsor this initially. The answer is, absolutely yes. And how can I possibly prove that? Well, we turned the internet on, on January 1st, 1983. Okay, do the math. How long ago was that? 1983. 32 years. Now, who do you suppose was actually running it at that point? It wasn't the Defense Department. I was sitting-- Actually, I had left the Defense Department. I was off in MCI doing MCI Mail at the time.

But my colleagues were parts of universities. They were in the private sector running, building and operating pieces of the internet. And it's been that way ever since. It has always been the private sector's role to build and operate these pieces. Of course the Defense Department has pieces of its own. So does the National Science Foundation and the NSF still. Well, NSF doesn't run the NSFnet anymore. They actually started it in 1986 and then they shut it down in '95. So they didn't need it anymore, because there were commercial services available.

The private sector and the civil society and the technical community and the academic community and governments all have a responsibility, including you, to be part of the policymaking apparatus for the internet. The things that you do to protect your own safety and security and privacy affect me too, because if you don't do a good job, then you become an avenue through which attacks can be made and, you know, phishing attacks occur, and access to things that shouldn't be accessed by their own parties will happen.

So we all have this shared responsibility to make policy decisions about the internet. The enforcement of policy could be the responsibility of specific organizations and individuals and the like. But the policymaking things should be multi-stakeholder. And, as far as I can tell, that has been working for the last 32 years. And it can continue to work if you just let it.

Next question.

JOHN HUGHES: Several questions about hacking. And the White House, the State Department have had networks hacked. Will there come a day when such hacks are not possible? And someone else wonders, who is responsible for cyber security? Who ultimately can stop the hacks from happening?

VINT CERF: So the answer lies in the previous response as well, because we are all responsible for improving the safety and security of the internet. Your own choices, your practices, the practices of the internet service providers, are all part of this fabric that we have to maintain.

There is a visual model I have in my head. Imagine that you have a set of homes whose backyards are all shared, you know. So there's this big kind of park. And the front doors go out this way, going outward. And imagine that there is some nincompoop who insists on leaving his house unlocked. So even if everybody else locks the house, this one guy lets people into the interior. And that's a risk, potentially, for you.

So I see the internet as having this character that we all have a role to play to make it more secure and safe. There are different places in the internet's architecture where attacks can be launched. So this is a very layered system. And so the mechanisms that might work at one layer may have no effect at another. I'll give you an example.

Suppose somebody says, "The solution to the email problem is that we should encrypt everything. And so, as long as we encrypt the email as it goes through the net, everything will be okay." Well, okay. Let's analyze this a little bit. The source of the email is using a laptop which has become infected somehow. Maybe they plugged in a USB that was infected, or they stuck in a DVD, or maybe they went to a website that had malware onboard. So this computer, which you don't know, or the user doesn't know is infected, composes a piece of email which has malware in it.

Then we encrypt it. It's great. So it goes all the way through the net. And nobody can see anything because it's all encrypted. It gets to the other end, it's decrypted, and that piece of malware does it damage. So crypto, at one level, does not necessarily solve all the problem. We have to put-- We have to put prevention in various layers in the system using various sundry technologies.

So, in a very-- I know this is kind of an oddball answer here, but it's sort of everybody's responsibility to do this. But each layer and each provider of service at those layers has a responsibility, just as we do at Google. We're way up in the application space. And we're doing everything we can to protect against the kinds of attacks which could be launched against our layers of the architecture. But there are other layers below us, the ones that are doing transport, that also need to contribute to the safety of the system.

JOHN HUGHES: Right now we use social and credit history to verify our legal identity. If Social Security Numbers didn't exist, what would identity verification look like? And is there a better way to do identity verification?

VINT CERF: Short answer is yes. Would you like me to elaborate? [laughter] So first of all, Social Security Numbers were not intended to be identifiers used in commerce, right. But you know, they are-- Or the last four digits, which is almost worse. Second, the Social Security Numbers don't have any check digits in them or anything.

There is no way to tell whether this is a valid or invalid Social Security Number. It's just nine digits. So we could do a lot better, especially with today's technology.

One possibility would be to issue a certificate which identifies a public key that belongs to you and to you alone. And what you would want is to have the private key that goes with it. And this is public key crypto stuff. This weird thing that my friends Marty Hellman and Whit Diffy[?] came up with in 1977, is kind of like a door with two locks. You have two keys. One key locks the door, but it doesn't unlock it. The other key unlocks the door but it doesn't lock it. And so you have these two different cryptographic keys that work together to create security.

So you can imagine having an identifier that has been digitally signed by an authority that would issue those identifiers. That authority could be a state government, because that's where the SSNs come from. Or it could-- Well, I guess it's the federal government. But the states issue these things by-- Does anybody know the answer to that? Is it correct that the states issues the Social Security Numbers, but they do so on-- The federal government does it. Okay, thank you.

So the federal government could issue these certificates. And as long as the digital signature works, this is a way of validating yourself remotely. Somebody could send you a challenge saying, "Are you really Vint Cerf with this public key?" And, if they encrypt that in my public key, only I can decrypt it in my private key. Just like the only guy who can unlock the door with the private key. And then I can send a response back to that party's-- using that party's public key to encrypt the response.

So we can verify that each of us has a credential issued by the federal government that has a public and private key associated with it. It's more complex than that. But we don't have time to go into all the details. But that's the essence of what could happen. It would be a lot better.

By the way, here is another opportunity for policy. If we could agree on an international basis about the bona fide days that have to be shown before you get one of these credentials, then we might be able to make a digital signature as significant and as authoritative as a wet signature is today. But we have to agree, on a global scale, what bona fides have to be presented in order to get this authorizing digital signature and certificate. I think that would be a really good thing to do, because it would encourage ecommerce. And it would also give us some protection against the abuse of our Social Security Numbers. So that's the long answer.

JOHN HUGHES: In addition to printing out our photos, what else should we as a society be doing to preserve information? That is, preserve our culture for future generations?

VINT CERF: Oh, that's a great question. I really didn't say print everything. But some people who are in the business of printing photographs decided that's what I said. [laughter] And, you know, you can't blame them. You know, printed photography has gotten kind of, you know, different from all of the stuff that you see on Flickr and everything else.

So here is the problem. Every single day, when you use software in your laptop or desktops and what have you, you create complex files. If you're using a text document editor, Microsoft Word or something else, the file that you create is actually a pretty complex object. And, in order to correctly render it or allow the document to be edited, you need a piece of software to help you. That's the application program.

Now I want you to imagine that it's the year, you know, 2150. And you're Doris Kerns Goodwin's, great, great granddaughter. And you want to write about the beginnings of the 21st century. Now remember, Doris Kerns Goodwin wrote that wonderful story about Lincoln and his team of rivals. If you read it, I hope you have the same reaction I did. The dialogue seemed very plausible. The opinions that were being stated, and the words that were being used, made it seem like she must have been a fly on the wall 150 years ago. Of course she wasn't.

She went to 100 different libraries and collected the physical correspondence of the principals and used that to reproduce the dialogue of the time. Now imagine it's 2150. You're Doris Kerns Goodwin's great, great granddaughter. And you're trying to write about the beginning of the 21st century. And you can't find a damn thing, because all the email has evaporated. Or, worse, you have these giant discs full of bits that represent the email. But the application program and the operating system it ran on, and the hardware that the operating system animated don't work anymore. They're gone. Nobody has supported them. You have a pile of rotten bits on your hands.

So I want to prevent that from happening. And there are only a few ways that I know of to do it. The best one that I have seen so far, I lectured about this with my partners at Carnegie Mellon just last week at Stanford University. This guy, Mahadev Satyanarayanan-- I practiced so hard to say that-- we call him Satya for obvious reasons. Satya has developed a virtual machine capability that will allow him to emulate hardware of pretty much any kind, and then run the operating systems on that emulated machine, and then run the application on the emulated operating system. And it works. He demonstrated. This is not slideware. He showed 20 different emulations of different machines and different operating systems. And my God, he was showing me 1997 TurboTax running on a Mac. And it looked, you know, including the crappy graphics and everything else. It was really a phenomenal performance.

So the ability to preserve software applications and operating systems and emulate the hardware is exactly the best answer, so far. Imagine running those emulations in the cloud, so that those machines are available to anyone. This is not a trivial technical problem. And also, there is intellectual property issues. How do I get a hold of the software? What rights can I get? What if I have the object code and I'm running it on the cloud, and somebody says, "You can't do that because they didn't pay"? And they said, "It's 150 years since you did anything with that software, you know. Give me a break."

You remember what happened when the Xerox machines were created and the librarians said, “People should have the right to copy a limited amount of material this way.” And the publishers were saying, “No, no, no. People will-- I’ll publish one book, and people will make Xeroxed copies of it, and I’ll never make any money.” Well, that didn’t happen. And this ability to employ fair use was very important. We need a preservation use like that, associated with copyrights, so that preservation, as an act, is not only sanctioned, but encouraged, so that our digital content will survive over long periods of time. That’s my long answer to that question.

JOHN HUGHES: We combined a couple questions here. In 1979, Bob Kahn urged you to create a brain trust in case you got hit by a bus and couldn’t continue your work. Who do you view as the brain trust today? And part two of that is, do you feel there is enough technical expertise or even consultation with technology experts among those who craft technology policy? So who is the brain trust? And is the brain trust being consulted like it should in technology policy?

VINT CERF: Okay, so the answer to the last part is no. The answer to the first part is that the original group that I created at Bob’s request was called the Internet Configuration Control Board, ICCB. We made it as boring as possible so nobody would want to be a member of that Board. And then, I appointed the people who were the lead researchers on the development of the internet at multiple universities around the U.S.

And so the ICCB morphed into the Internet Activities Board around 1984. It later became the Internet Architecture Board in 1992, when it became part of the Internet Society. And now Internet Architecture Board and the Internet Engineering Taskforce and the Internet Research Taskforce, all of which are housed in the Internet Society, are the brain trust for the technical revolution of the internet. That’s where the bulk of the new protocols are coming from.

This is not to disenfranchise various corporate entities that are trying to develop new protocols and new applications for the net, but the core of the internet’s evolution still comes from that brain trust. I have lived here in Washington since 1976. And I've considered it to be both a privilege and a responsibility to try to help policymakers understand enough about the internet so the policies they make makes some sense. And, you know, I'm not looking for technical depth here. I'm looking for simple cartoon models of how the network works, that are accurate enough so, if you reason with those simple models, you will reach the right kind of conclusions about what policies are implementable and which ones are not.

The last thing you want is a policy that requires you to double the speed of light, for example, or abandon the law of gravity. So our job as technologists, I think, is to try to be helpful, to provide clear enough explanations for how this stuff works, so that when policy gets developed, it actually is implementable and it makes sense. And the worst thing in the world is to pass laws that can't be enforced or can't be implemented because it encourages disrespect for the law. And that’s not a good thing.

JOHN HUGHES: Looking over the past two decades or so, what are the one or two developments in the internet that you are most pleased with and most disappointed with?

VINT CERF: Well, starting with the last one, spam is a kind of a disappointment. [laughter] And I have to say, I'm very proud of my company, Google, because we've done a very good job of filtering out an awful lot of spam. And if you happen to be using Gmail, if you ever looked at your spam folder, it's amazing how much stuff you didn't have to look at, especially, you know, how to enlarge body parts and all that stuff.

So that's-- It's an annoying side effect that email is essentially free. So it means the spammers don't get-- don't have to pay for what they do. And there are crazy ideas like, you know, charge 0.002 cents for every email. It's not enforceable, so forget that. So spam is annoying, but there are ways of filtering it out.

The thing which I was most astonished by-- proud is a very funny word to use here. In fact, let me go down an alley for a moment. Some of you have kids, right? And you might have learned what I learned, which is don't take too much credit for when your kids do well, so when they screw up you don't have to take too much blame. [laughter]

And so, you know, I think that-- proud is the wrong word to use about internet. I'm just grateful to have been part of this story. However, with regard to surprises, when Tim Berners-Lee's worldwide web showed up in 1989, nobody really noticed except Tim and some of his colleagues at Cern. But, when the mosaic browser showed up around 1993, this was absolutely astonishing, because it turned the internet into a magazine. It had imagery and color. And it had formatted text. It was really quite eye-opening.

On top of that, the browsers had this feature that, if you wanted to see how the web page was built, you could ask the browser to show you the HTML, the HyperText Markup Language. So this was open. Everybody could copy everybody's web pages. And they did. And then they found new ways of making them more interesting. So you know, the webmaster was a kind of a role which didn't exist before the worldwide web. And it was sort of enhanced by the fact that everybody could share each other's web pages and how they were built.

And so the thing that astonished me was the amount of content that poured into the net once the web browsers and HTML were available. It was just astonishing how much information people wanted to share. Not because they wanted to be paid, but they wanted to know that their information was useful to somebody else. And so, you know, you hear this story about information is power. Nonsense. It's information sharing that's power. And we've seen it. And we've seen it over the past 20 decades-- or 20 years. And we're going to see it over the next 20 years, maybe the next 20 decades too.

So the thing that I like the most about the internet is that it is evolvable. It is scalable. It's well over a million times bigger than it was when we turned it on. There aren't too many protocols that will allow you to do that kind of scaling. And it has invited creativity. We use the term “permissionless innovation” very deliberately. You don’t have to get permission from every ISP in the world to invent a new product or service and put it up on the net. And it should stay that way.

JOHN HUGHES: This questioner says, you are said to have been a candidate for the Office of U.S. Chief Technology Officer. And wants to know if you would have taken that job. But really, a larger question also is, would you consider moving over to the government side to help sort out some of these issues in some kind of senior role, if offered?

VINT CERF: Wow. So this a hypothetical, Mr. Chairman. So first of all, the answer is, there were news reports that I might have been on the list. I don’t actually know. But I consulted with some of my friends, including Eric. And Eric said, “You know, why don’t you just be the Chief Technology Officer’s best friend?” And so I made good friends with Anish and with his successor and, of course, Meghan, who is now there as CTO. And I thought that was pretty good advice.

Now, I have served in the government. I served six years at DARPA. I really enjoyed that time. It was an empowering moment for me. It was a period of time that where I worked with incredibly smart people. But my whole career has been that way. I mean I'm at Google, surrounded by incredibly smart people, most of them are smarter than I am. And I learn that every single day, especially when the 25 year olds run over and say, “Why don’t we do X?” for some value of X. And I’ll sit here thinking, “Oh, we tried that 25 years ago, and it didn’t work.”

Then I have to remember that 25 years ago, there's a reason why it didn’t work. And that reason may no longer be valid. It could be that computers are cheaper, they're faster, there's more memory, something else is economically feasible that wasn’t before. I have been forced to rethink my own views on these things over and over and over again. And let me tell you, nothing keeps you younger than having to rethink your own positions instead of falling into a rut.

So for me, I think I don’t feel the need to become part of the government. But I want very much to have an opportunity to provide support and help if I can. And I will do that if I am allowed.

JOHN HUGHES: Do you want to see Congress pass the USA Freedom Act? And Congress just had a hearing on encryption, focusing on privacy rights versus law enforcement’s desire for a backdoor into cell phones, etcetera. What do you think Congress should do?

VINT CERF: Well, so first of all, this backdoor idea is indicative of a real tension here. I mean this global system is used and abused like a lot of technology. There isn't anything about the technology that determines whether or not it’s a constructive or destructive use. It’s just a neutral tool, and some people abuse it.

And so we have to do something. I mean we wish to protect the citizens of our country and others from harm in this network. And so you'll have to ask yourself, well how can I do that? What steps can I take? And the tension, pretty obviously, is that if you use things like cryptography to protect privacy and confidentiality, which I'm sure everyone of you cares about, there is this question about, what about the law enforcement people? And what can they do?

And the proposal to put backdoors into things is reminiscent of something else some of you will have reported on, the clipper chip, back in the '90s. I was absolutely adamantly against the clipper chip idea. And the reason was very simple. If you have a backdoor, somebody will find it. And that somebody may be a bad guy or bad guys. And they will intentionally abuse their access.

So creating this kind of technology is super, super risky. And so I don't think that's the right answer. Now, at the same time, I accept that governments are there, in part, to protect their citizens from harm. So the question is, how do you do that? And there is this spectrum. Imagine that, on one end, we live in a society where there is no privacy at all. Everything is known. Everything you're planning to do is known. It might be a very safe society to live in. But it might not be one that you want to live in.

On the other hand, what about a society where there's absolute privacy. Nobody knows what you're planning to do at all. And bad stuff happens. So you feel that your privacy is protected, but your safety has now been diminished. There must be someplace in between. And it isn't the same place for everyone. It isn't the same place for every culture. And it isn't the same place for every nation. Our job in the U.S. is to figure out, where is that balance for us?

And I think the Congress is forced, now, to struggle with that. And they're going to have to listen to these various arguments about protection and safety on the one hand, and preservation and privacy and confidentiality on the other. I'm not persuaded that building backdoors is the right way forward.

JOHN HUGHES: The way the FCC's Title II Net Neutrality Rules are written, do you think they offer equal opportunity download speeds while forbearing enough Title II Rules to avoid government overreach like new fees or content regulation?

VINT CERF: So this is a really interesting problem. And some of you have lived through this for a couple of decades. I think that Tom Wheeler didn't have a whole lot of choice. The FCC had asserted a set of neutrality rules which were intended to protect user choice. And they were essentially told by the Supreme Court, "You do not have the legal basis to enforce your network neutrality preferences."

And so I think Wheeler had three possibilities. One, do nothing, in which case the net neutrality notions, to the extent that people agree that they are helpful and useful and preserve user choice, would simply not succeed because of the lack of legal basis for

FCC's enforcement. The second possibility would have been to get the Congress to create a new title in the telecommunications act specific to internet.

Now some of you will remember, there was a brand X decision. This is the cable companies and the telephone companies were saying, "We are not regulated the same way." This is correct. There's two different titles in the telecom act for dealing with these two entities. And yet, they were both providing internet service. And the complaint was, "We're providing internet service under different ground rules. This isn't fair."

So the question is, what to do? One possibility might have been, get the Congress to adopt an internet title that was appropriate to the internet technology. The choice that was made, instead, was to treat internet as if it's just an information service that had no layered structure, it had no telecommunications component. It was just an information service, end of story.

Well that led to-- That's an unregulated title. And so the FCC rule was completely removed. Tom chose a third path. And that was to invoke the Title II, which had been-- The FCC had the authority, in my view-- remember IAML, right. But I believe they had the authority to decide it was Title I. They have equal authority to decide, "No, no, it's really Title II," but constrained significantly.

So what's the issue here? Well now, under this current rule, they have a basis for taking action if they think that the neutrality rules have been violated. However, there is this potential forward-looking risk. What happens if some new FCC in some future game decides to invoke all of the messy complexities of Title II, which were designed for a system for voice communication, which is a far cry from today's internet and probably very much a far cry from tomorrow's internet.

So at some point, this tactic probably has to be readdressed so that we, if we're going to do anything at all in the regulatory space, it needs to be tailored to a network which I want to emphasize again must still be evolvable, it must be possible to add new products and services to it. We should not constrain the network, you know, simply in order to regulate it. We need to find a way to make sure that the network is fairly-- treats you fairly, gives you adequate opportunity, incites competition, but at the same time, allows the FCC to protect your interests. So that's where my head is. And I hope, as a former Congresswoman that you think I managed to straddle this reasonably well.

JOHN HUGHES: I mentioned in the introduction that, at the National Press Club, we fight for press freedom worldwide. And part of your job is evangelizing the internet worldwide. What do you say to governments and regimes who consider the internet a threat? And what can you do to try to shake that loose?

VINT CERF: I wish I could just say get over it. But that doesn't work. Let's take-- Everybody picks on China, so I guess I'll do that too. But they are a good example of a tension. I actually have some sympathy for the Chinese government. You realize that there are 650 million Chinese on the internet now? That's like over a third of their-- well, yeah, more than a third of their population, close to half. And so this means that the Chinese government and the private sector there have been investing an enormous amount in building infrastructure for the internet. Fiber networks they were very early on into the IP v. 6 space, by the way, you know, bang, bang. So yeah, this is even better.

So they have made this big investment. At the same time, they come from a long history of very authoritarian practices. And so they're scared, frankly, about this large population of people becoming unhappy. And, if you study Chinese history, which I have not, I am told that the last seven times there was a major regime change in China is because it was preceded by a peasant rebellion. And looking at all of the conditions throughout China, especially on the west, you can appreciate that things are really, you know, scary for the administration, even if they're trying to do the right thing, which is to make sure people are fed and housed and everything else.

So my story is that the countries that are seeking authoritarian control over the internet will discover, at some point, that if they do that, they're shooting themselves in the foot. First of all, they're potentially inhibiting the creativity of the population, which is what they need in order to improve GDP. Second, they may be inhibiting their ability to explore world markets. And I don't care what country you are, even the U.S. The global economy is bigger than you are. Don't cut yourself off from access to it. The same message needs to get to the Europeans who were struggling with the digital single market. But you know, at the same time, may be accidentally preventing themselves from participating in a global market, and letting the global market participate in the European one.

So my message has always been economic. It is in your interest, Mr. President, to invest in the internet, to keep it as open as possible, and to allow your creative population to make use of it. No country has a corner on creativity and invention. It's uniformly distributed throughout the population of the world. It's just that the people with these ideas don't always have the wherewithal and the support in order to explore those ideas.

And I will give you, as a concrete example of that, how many folks come from India to the Silicon Valley or Seattle or here and do spectacularly well? Their ideas were the same. It's just that they didn't have the investment infrastructure, the willingness to take risk that we have in the United States. And so we know that there are smart people out there with the possibility to improve their own GDP if the rules could be made similar to what they are here in the United States.

JOHN HUGHES: We are almost out of time. But before I ask the last question, I'd like to remind everyone about some upcoming speakers. Lieutenant General Michelle Johnson, the first woman to lead the Air Force Academy, will address a Luncheon on Friday. The CEOs of American, Delta and United Airlines will appear together at a Luncheon on May 15th.

VINT CERF: What an opportunity. [laughter]

JOHN HUGHES: And Garrison Keillor, author and host of Prairie Home Companion, will address the Press Club on May 22nd. I would now like to present our guest with the greatest gift of all, the National Press Club mug, which you can treasure for decades.

[applause]

VINT CERF: Mug shot! That is a mug shot.

JOHN HUGHES: And now the final question, maybe we have time for two, depending on how long your answer is.

VINT CERF: How long my answers are.

JOHN HUGHES: Yeah, yeah. This question almost sounds like it could have come in over the internet. I'm not sure whether it did. This questioner says, you have fewer than 5,000 followers on Twitter. And you're not verified. What's up with that?

[laughter]

VINT CERF: So I don't tweet all that much, just every once in a while. You know, I have better things to do. And besides, I get more than enough visibility as it is. I don't need anymore. I mean I got stopped by two autograph guys, right, as I walked in today. And I don't know, verification, what do you have to do to get verified? Send your blood type or something?

JOHN HUGHES: We'll have to ask Twitter.

VINT CERF: Oh, I remember asking the guy that started Twitter. He says, "Is your title Chief Twit?" He didn't think that was very funny. [laughter] Next question.

JOHN HUGHES: Why isn't there a Nobel Prize in computing? And should there be one?

VINT CERF: Oh well. You know, you'd have to ask Mr. Nobel. But he's long passed. The story, which may not be true, is that Mr. Nobel's wife ran away with a really good mathematician. And in consequence, Mr. Nobel told his committee that, under no circumstance, will any branch of mathematics be recognized by the Nobel Prize. And unfortunately, computer sciences tended to be associated with mathematics, understandably. So we in that field are not eligible for the Nobel Prize. We might be eligible for the Peace Prize, but that's a real stretch, because that's a very political kind of thing.

There is, however, a prize that's offered by the Association for Computing Machinery, which was founded in 1947 in the U.S. It has now gone global. There is a Chinese and an Indian and European Council in addition to the one which oversees the whole global operation. I am former President of ACM. I'm still serving in that role until the middle of 2016. And the prize is called the Turing Award, named after Ellen Turing. Many of you, by this time, will know from the movies that have been made. That prize is $1 million dollars. It’s funded by Google. And we’re proud to offer that through ACM every year. And I did get that prize, along with Bob Kahn, in 2004. So I feel more than adequately compensated. It wasn’t a million dollars back then. And they aren't doing it retroactively. [laughter] I asked, but that didn’t work. So it’s a coveted and very high recognition of contribution to the computer science community. I think that's more than enough.

JOHN HUGHES: How about a round of applause for our speaker. Thank you very much. [applause] I would also like to thank National Press Club staff including its Journalism Institute and Broadcast Center for organizing today’s event. And remember, if you would like a copy of today’s program, or to learn more about the National Press Club, go to our website. That’s press.org. Thank you very much. We are adjourned. [gavel]

END