Google's Eric Schmidt and Jared Cohen

https://www.climateone.org/audio/googles-eric-schmidt-and-jared-cohen
Recorded on June 4, 2013

Greg Dalton: Welcome to the Commonwealth Club, where you are in the know. I'm Greg Dalton, host of Climate One, the Commonwealth Club Sustainability program.

Today, we're discussing the digital future with Google's Eric Schmidt and Jared Cohen. The rapid spread of mobile phones connected to the Internet is impacting economies and societies all over the world. By 2025, the majority of the world's population will have unfiltered access to all of the world's information through a device that fits in the palm of the hand. In the next hour, we will discuss how information technology will influence the balance of power between citizens and states, its increasing role in national security, and the privacy price that people pay to be part of online culture.

Along the way, we will include one or two audience questions submitted in advance via YouTube and questions live tweeted by some of the 600 people in the audience with us today. We also will include questions submitted on communication technology that's nearly 2000 years old -- paper.

Eric Schmidt is Executive Chairman of Google and co-author of The New Digital Age: Reshaping the Future of People, Nations, and Business. He previously served as CEO of Google and has a PhD in Computer Science. Jared Cohen is Director of Google Ideas, the company's think-tank based in New York, and co-author of The New Digital Age. He was a Rhodes scholar and previously served under the U.S. State Department's Policy and Planning staff under Secretary of State Condoleeza Rice and Secretary Hillary Rodham Clinton. Please welcome them to the Commonwealth Club.

[Applause]

Greg Dalton: Welcome. Thank you for coming.

So, Eric Schmidt, the focus of this book is that new information technology and history has often challenged the establishment, the state, the government, the elite. So how is that happening now with new mobile phone technologies?

Eric Schmidt: Well, Greg, let me start by saying -- by thanking you for hosting this event. When I was a graduate student at Berkeley, driving to Xerox Park where a lot of the computer technology we use today was invented, I listened to a radio show every time I went back and forth, which was this show. And I dreamed one day of being in the audience. I understood the reach of what the Commonwealth Club meant. So now, 30 plus years later, we're all here, and it's still that important as a dissemination vehicle, which is why we chose this for our San Francisco book tour. So thank you all for being here.

[Applause]

So, Jared and I started talking about this a couple of years ago. We couldn't quite figure out where we're going to come out. But we made some observations, and I think one of them is that the Internet is going to wire up the entire world. There are roughly 3.4 billion phones in use today -- actual phones in use. There are more than a billion smart phones of which 900 million are Android phones, thank you very much. And as those numbers increase and as the next five billion join the Internet, they are going to do it with mobile devices.

So for us in the developed world, the future is fantastic. All of a sudden, new services will emerge. Think of them as a perfectly intelligent digital assistant who can assist you in planning your life and helping you out in every conceivable way. And you're going to love the products that Google and many other companies here in California are going to produce, as well as globally.

But the change to people who have no information, no political freedom, no health care, no access to entertainment, when that mobile phone comes up, it's going to be extraordinary. It's going to be such a greater change. And of course in the book, so we sort of took that as a view, and then we began to explore the question, Greg, that you mentioned, which is what will people do and how will societies change. Now, the Internet comes with some questions. It comes with some issues -- whether they're privacy or the impact on terrorism, or in particular, how governments will behave with this new shift of power to individuals.

Greg Dalton: Jared?

Jared Cohen: And just to add to this, one of the reasons we decided to write this book is we were sick and tired of this debate that dominated the present around is technology good or is technology bad. While this debate is intellectually interesting, it completely ignores the inevitability of it, that Eric spoke about.

So when you think about five billion new people coming online, you also have to think about where they are coming online. These are parts of the world where there's conflict, instability, where the governments are repressive. Now, we point out in the book that 57 percent of the world's population lives under some kind of autocracy. So, one of the things we tried to do is we traveled to 30-plus countries around the world, largely places that are unstable and autocratic, to try to meet some of these future users who are coming online and understand how their challenges are different from the two billion who are already connected.

So we went to North Korea, we went to Libya, Afghanistan, Pakistan, and a number of other places. And we found a number of similarities in terms of how they use the tools and similarities in terms of some of the challenges that they face. But we also found a whole different set of issues that these vast majority of our future users are going to encounter. And it's startling to think that these are the environments where the majority of people using technology are going to live. So we started asking questions: what does this mean for the future of dictatorships and autocracy; how will this transform the terrorist threat that so many of us are worried about and that keeps us up at night? And in the book, we attempted to sort of predict and answer some of these questions.

Greg Dalton: And you write about Egypt, for example. There's a case where the state was using -- during the Arab Spring, there was some uprising. Social media has been a factor and Egypt tried to cut it off, and that -- how did that work out for them?

Jared Cohen: Well, I was in Egypt the day the revolution happened. And by the way, one sort of side note; I went to go see the pyramids before the revolution -- sort of the day the revolution began -- and everybody knew it was going to start at one o'clock. And literally, people, when I got back from the pyramids, were like slowly sort of making their way out of bed to get ready for the revolution. What was interesting is going on to the street and talking to young people. You know, the assumption is they're all there because they hate Mubarak and have some sort of long-standing grievance against him. And in fact, some of the people you talk to have that belief. But then a lot of the younger people that you talk to, what they would say to you, "Look, I didn't like Mubarak. Life wasn't great here. It was hard for me to be political. But I wouldn't have gone to the streets and risk having stones thrown at me or risk getting shot. But then he shut down the Internet and he shut down mobile devices and he really pissed me off."

[Laughter]

So you have all these young people going into the streets. Now, it's extraordinary…

Eric Schmidt: And plus, they had nothing else to do.

Jared Cohen: Well, because they would complain that they were sort of sharing a room with their siblings and that it was hot…

Eric Schmidt: The Internet was the great time-waster and they took it off.

Greg Dalton: So what does this mean -- what was the lesson for other dictators out there watching this?

[Laughter]

Jared Cohen: Yeah talk about a dilemma…

Eric Schmidt: The dictator's dilemma. We like to give dictators, you know, dilemmas. One of the interesting -- well, first place, it's clear that if you're an evil dictator, and raise your hand if you're a member of that class. This gentleman over here raised his hand. Get to know you a little bit better. You don't shut down the Internet; you censor it. You filter it. You try to make sure that information that would get the people riled up is not available to them.

It's remarkable how happy people can be when they're ignorant of things that they really should be caring about. When we were in North Korea, I figured that, boy, the people would be fighting in the streets and knives and so forth. But, in fact, people got up and went around their business. So it's the lack of information that is the ultimate tool of dictators.

We're about to run this test tomorrow in Turkey. The prime minister has announced that the demonstrations, which are largely around land control and development and sort of, shall we say, inclusiveness of discourse and power, he's announced that the demonstrations have to stop tomorrow by the time he lands in town. So we'll see. Keep your eyes open. Maybe we'll have another test; maybe we won't.

Greg Dalton: These technologies can also be used by dictators to monitor and suppress. So talk about the shadow side of these technologies. Jared Cohen?

Jared Cohen: There's one important point that gets to that question but also adds to what Eric is saying, you know, in the spirit of this dictator's dilemma. And let me sort of preface what I'm about to say by asking all of you a simple question: how many of you, by show of hands, have multiple email accounts? How many of you have multiple social networking profiles --

Eric Schmidt: That was essentially everybody.

Greg Dalton: Everybody in the house.

Jared Cohen: Multiple chatting passes -- et cetera. You guys get the idea. So basically, in the physical world you're one person, but online you've got a whole virtual entourage of yourselves. So maybe, you know, one member of that entourage like misbehaves and does shady things and other one is sort of useful for professional reasons. It's the same thing in --

[Laughter]

Eric Schmidt: Your good and bad alter-ego.

Jared Cohen: And by the way, you all know this is true. So, in autocratic environments, it's the same thing. So let's -- Iran. Iran is going to have a presidential election in just a few weeks. The country is 72 million physical members of the population. In the future when every one of them is online and they would all raise their hands just like you all did, online, that population is going to look more like 500 million people. And so the dictator's dilemma in the future is distinguishing between what's noise and what's actually real.

How do you know that when there's sort of a disturbance online that it's not just 10 people acting like thousands? And where they overreach and overreact, they run the risk of taking something that is digitally robust and pushing it into the streets.

Eric Schmidt: How do you know -- the old issue in the Internet is how do you know -- it's a dog versus a person. But how do you know that these are real revolutionaries that are threatening your dictatorship versus people who are just having a good time yelling about you? One of the things we talk about in the book is one strategy for the dictator would be to allow for expression the physical space -- in the virtual space, but shut off any expression in the physical space, right? So you have choices as a dictator of how you do this.

What we ultimately however concluded is that it's better not to be the dictator side, because these tools are so empowering of individuals, and it's so easy for people to go around these kinds of surveillance systems using various techniques including cryptography, that you really -- if you really want to be a dictator, you really don't want to have the Internet around. It's too empowering of the citizens that you're not serving well.

Greg Dalton: What you just said is that people have more liberty in virtual space than they do in the real world. Is that what you -- in the physical place, there's higher constraints than there is in the virtual world?

Eric Schmidt: No, we're suggesting that that may be one of the strategies that dictatorships are -- authoritarian regimes do. One of the estimates is that 57 percent of the world's population that's coming online lives in authoritarian or essentially un-free environments. They don't have the same expectations that we do. They don't expect the rule of law to apply. They assume the police are corrupt. They have no expectation of privacy. And so for them, this is a very strong empowerment device.

Greg Dalton: You've just described China pretty well. So this week, there's a presidential summit between the president of China and the president of the United States. Cyber-espionage, cyber-warfare is on the agenda. What do you think is going to happen? How do think that's going to -- you write about the new "Code War" as a successor to the Cold War.

Eric Schmidt: We spend a fair amount of time talking about the possibility of cyberwar, and the sort of conclusion you come to is that there's going to be low-grade fighting, if you will, between countries, for a very long time in cyberspace. China is a classic example. By all accounts, America has a good relationship with China. Among other things, they buy our debt, we buy their products. There's a tremendous amount of trade back and forth. It's mutually beneficial in most of people's eyes.

And yet on the Internet, it's a completely different story. Not only are they filtering and censoring the Internet, but they, among other things, attacked Google -- I mean who would have thought? -- along with many other countries, and off the unscientific survey of the level of attacks indicates that

majority of the source, 80-ish percent, are originating in China for whatever reasons.

So you can imagine the following scenario: the Chinese military -- and think about "Dr. Strangelove," right? A Chinese military guy decides to have a little fun, and so he releases a virus into America. And that virus, by the way, mutates in some way that it actually causes some physical damage. Some bad stuff. And this could happen.

So now what we have is we have, in the summit, we have the Chinese premier says, you know, "Mr. President, Barack, sorry, we didn't authorize this and this time I'm telling you the truth." What's the president going to do? Actually, I mentioned to President Obama and he sort of looked at me, "Oh my God." You actually have to think about these things, right? You want to think about them before they happen. Now imagine the same scenario, but because of the lack of attribution on the Internet, it's really from another country and they've set it up to blame China. And these poor Chinese people really are not guilty of this. And the Internet has some properties. It's hard to attribute where the things come from. It's possible to do a lot of damage at least digitally, and our systems are not fully protected of it. There's a lot of reasons -- here, for example: how many of you know that the Chinese and others are not inside your corporate or university networks? Raise your hand if you're sure.

Greg Dalton: No one's sure. One of the FBI's main jobs now in the Bay Area is to look at this kind of espionage. Jared Cohen, let's get you on the cyber-espionage.

Jared Cohen: Yeah, so let me make a larger point about sort of the cyber-attacks that are going on and then some things specific about China. You know, one of the things that we write about in the book, and we're very concerned about, is we often talk about, you know, cyber-terrorism and cyber-war in one silo and physical world terrorism and physical war in another silo. So people talk about and speculate about what a cyber-Pearl Harbor might look like or what a future 9/11 might look like, but we have to sort of resist the urge to silo these things, because, at the end of the day, what we should really fear is coordinated attacks across both domains, or a situation when a cyber-attack is so severe, it warrants a physical world response.

Eric Schmidt: Jared, one day -- you announced you had thought about what would be the most terrifying attack is really the combination of these two. Can you give us a scenario where that could occur?

Jared Cohen: Well, I think it was -- once we got mobile coverage back in --

Eric Schmidt: Look, we spent six months together, Jared. You must remember some of these things.

Jared Cohen: Well, I know. And I do -- I remember after Hurricane Sandy, you know, sort of turned downtown Manhattan into "little North Korea," quoted Jon Stewart, I called Eric and I said, "This is really terrifying not because of what national disasters and hurricanes can do, but this is sort of a forecasting of what a really terrifying terrorist attack could accomplish."

So you could imagine the situation where a cyber-terrorist attack takes out the electricity of a major city, paving the way for a couple of terrorists to physically go in there and do something terrible undetected. It is a very real scenario.

Eric Schmidt: And we obviously think this is a terrible thing; we're not endorsing it in any way. The possibility -- so you sit there and you go, "Well, how could this happen?" After all, these terrorists are operating out of caves. One of the things we talk about in the book, is you could imagine sort of a bad alliance between the criminal hacking gangs that exist, you get, you know, you

see these periodically online, and they have technical skills and they're after money, and these sort of evil terrorist groups. They could actually form a sort of super-group. It could actually be quite serious.

Jared Cohen: But if I can just go back to China, for a minute, not to pick on them but there's a lot of reasons to these days. Everybody talks about intellectual property theft and what the Chinese are doing with regards to restricting the civil liberties of their population, but there's a larger aspect of what China is doing internationally that has even more serious implications. And the best way to think about this is to understand that most of the world's technological infrastructure has not yet been built. And I'm talking about societies that are autocratic and a part of that next five billion.

So the question is, who's going to build out that infrastructure? There's only so many companies and so many countries that have the ability to do this. So what you have, for instance, Chinese companies that will have all kinds of trapdoors in their technology that lend themselves towards greater surveillance, helping the next generation of autocracies come online, or you have companies that are rooted in democratic values and democratic countries being the ones building that out. And this is why we talk about, you know, a future sort of cyber-code war where you have, you know, two types of countries or two types of companies competing to build out that infrastructure with very serious, lasting implications.

Greg Dalton: And one of the big four is Huawei, which is a big Chinese company. So is there a concern there about them? Infrastructure leads to influence?

Eric Schmidt: We don't know enough about what they're doing inside to have a technically correct answer.

So I think our statement is more be careful who the architects of your Internet are, because the architects carry some biases. The fact that the Internet was built in America, designed here in the good old USA and so forth, it carries a set of properties which we take for granted which are not common elsewhere. So the successive communications, the broad ability to distribute information, the inability to stop transmission, the lack of trapdoors, it’s a core aspect of how the Internet works, and it's something which governments will fight.

Greg Dalton: And you write about the possible balkanization of the Internet. Right now, it's kind of free flow everywhere, but it could become very different than we know it today.

Eric Schmidt: Well, you know, as we talked about it, governments do not necessarily agree that free and open speech, especially when it criticizes the government, is a good thing. There are roughly 44 countries that have one form or another of censorship or filtering, of which China is by far the most active. But, the others are learning quickly.

An example is that Bangladesh just issued an RFP, request for a proposal for their Internet so that they could do the same censorship. This is a country that's among the most -- the poorest in the world, and this is their concern? Russia passed what is essentially a child safety law, and, apparently, child safety includes prohibiting a great deal of criticism of the prime minister. Shocking. [Laughter] I didn't realize that they were hurtful the children that the prime minister be discussed in this way.

We've had situations where in Thailand, for example, there was a video that was not complimentary and not okay with respect to the king, so all of YouTube was banned. Now, is that because of the desecration of the king, which is illegal in Thailand? Was that because the military junta at that time did not want to have all those YouTube videos critical of them as they were misrunning the country.

That is now being fixed, by the way.

So again, governments' reaction is to shut things down. In Google's case, there's sort of a horrific video, known as the "Innocence of Muslims" video, which for various reasons, YouTube decided to keep up. As a result, a whole bunch of countries banned all of YouTube.

Greg Dalton: If you're just joining us on the radio, our guests today at the Commonwealth Club are Eric Schmidt, Executive Chairman of Google, and Jared Cohen, Director of Google Ideas. I'm Greg Dalton.

You also write about the news industry and how it will report less and validate more. So, how will this technology continue to disrupt the news industry? Jared Cohen?

Jared Cohen: Well, a lot of people like to make the argument that, "oh, the mainstream media is going away, et cetera." And that's not true. Obviously, the industry has challenges, and yes it's true that the sort of days of sending the truck and the sort of small number of reporters are out there to be on the scene before anybody else, you know, is being replaced by the fact that there's always going to be somebody there with a mobile device to catch it sooner and faster.

So then you ask, what is the comparative advantage that the mainstream media has, you know, that citizen reporters armed with mobile devices don't. And it's the credibility to validate and analyze. And it's ultimately up to every single media outlet to sort of how far are they willing to go without compromising their superior advantage with regards to the ability to do those two things. To go back to the Egypt example, another sort of interesting observation is you see all these people taking pictures of what happens, and then they run it over to a mainstream media outlet. Or wherever there's a crisis, you get lots of people with content, but ultimately, that content isn't real until some major media outlet says it's real. And that can be by broadcasting it, that can be by tweeting it, that can be by posting it, et cetera.

And so we argue that, you know, the mainstream media is not going away but there'll be this symbiotic relationship that exists between the people with mobile devices who will always have the content first, and the mainstream media that's needed to make it real and help amplify it.

Eric Schmidt: Yeah, but I mean we also say something very important. We say that you all will be subscribing to the Jay-Z news.

Jared Cohen: I thought it was Bieber news.

Eric Schmidt: Bieber news?

Jared Cohen: We fought about this, remember?

Eric Schmidt: We fought about this. I'm in the Jay-Z news camp.

Jared Cohen: I didn't say I was in the Bieber news camp. I just said it could happen.

[Laughter]

Eric Schmidt: You're Bieberlicious… Yeah. But what's going to happen is, you know, people are obsessed with celebrities. And you'll see a category of celebrities that will get involved in news-gathering. And you know, you can imagine Jay-Z's newspaper, you know, sort of urban attitude kind of coverage. And you can imagine lots of that. And the fact of the matter is that you're going to see many new trusted sources -- trusted in different ways -- but the sort of core ability to crowd-source

information will be, sort of, the instantaneous stuff, will be in the realms of places like Twitter.

You told me about this bizarre story that the Situation Room couldn't use Twitter?

Jared Cohen: Yes. This is actually an amazing story. When the White House got information that there was going to be a major uprising in Libya, they're all sort of told that Saturday to sort of stand by and they'll get a phone call if things started happening. And a friend of mine whose name I won't mention, a pretty senior official at the White House, on his couch, you know, had his tablet on his lap and was just looking at Twitter. And he saw that Richard Engel, the NBC reporter was sort of tweeting like crazy about, you know, how everything's just sort of become a mess in Libya, people are pouring into the streets. And so he calls the White House Situation Room to say, "Should I come in?" And they say, "What are you talking about?" He said, "Well, according to Twitter, Libya's like going off right now." And they said, "Let me check." And so they in fact checked and came back to him and said, "You're right. You should come in."

And the reason -- so basically, Twitter knew about this before the White House Situation Room, and the sort of ultimate consequence to this is now in the White House; they're allowed to view Twitter, they just can't post to it. You know, big steps.

Greg Dalton: Another aspect of the news business is leaks, and there's the trial of Bradley Manning started this week. The WikiLeaks has been a big thing. So how does that fit into your construct, this idea that secret government information can now be disclosed en masse?

Eric Schmidt: There are a couple comments to make about the Internet in general. The Internet lacks a delete button. And information that was secret that is released, such as WikiLeaks and others, once it's out there, it's not going to get redacted. You can't do it. And in that case, for example, the harder you try to prevent the release of that information, the more you stamp out copies, the more likely is somebody or some other country is going to make a copy of it. We saw this recently with the gentleman who thought he was being brilliant by releasing 3D printing prints for a plastic gun that can evade x-ray machines. The U.S. government ordered that information taken down, but by then, the information has been stored all over the world. So the secret is out.

We also went to visit Julian Assange when he was in his earlier form of confinement, and he made an argument, which I found pretty convincing, that if you're going to do systemic evil, the best way to prevent that is to leak it. Because systematic evil by governments, you have to write it down. We ultimately went to Rwanda where 750,000 people were killed by machetes, and we -- Jared's in fact an expert on that; he wrote a very important book on the Rwanda conflict. And you think about it for a while, and you think if they've known about it, they must have planned it at that level. And if those plans have been leaked or people had mobile phones, perhaps they would have prevented much of the genocide.

The problem that we had with that argument is who gets to make this decision. Does the leaker make the decision? Does the government make the decision? And it's not obvious to me how you make that decision but the principles are that information once released is very hard to put back. And so if you have something that's that important, you have to really think about who's going to have access to it and what their motivations will be.

And finally, you have think about if you're going to have systematic evil, how will you use leaking to police it and who is the appropriate person to police that?

Greg Dalton: Any thoughts on Bradley Manning?

Eric Schmidt: Don't know enough -- he's on trial now. It's probably better to let the process fall.

Greg Dalton: Jared Cohen?

Jared Cohen: If I can just jump in though on this question of data permanence, we sort of -- we frequently talk about, you know, data permanence in the context of once things are leaked, there is privacy and security, but it's interesting to think about data permanence in the context of criminality and terrorism -- two things that really plague our world today. And one of the arguments we make in the book is whether you're a criminal or a terrorist, in the future it's going to be very difficult to imagine any of them operating in a cave in Tora Bora. So if we assume that every terrorist and criminal will have to opt to technology to be relevant; ultimately, that's good for fighting crime and combating violence, because, by opting in, they're susceptible to leading a digital trail.

Eric Schmidt: Look at an example. In Boston, we got the two guys who killed the three people in a terrorist attack, car-jack a Mercedes with a Chinese guy in it, who doesn't speak very good English; they terrorized him for 90 minutes, drives around. He eventually escapes from the car. He leaves his cell phone in the car. So as a result of his cell phone being in the car, they were able to track the car, and they ultimately stopped the car -- one of the assailants was killed and another one was injured, leading him to the boat and everybody knows the history there.

So in the sort of evil terrorist manual, step number 27 is make sure there's no cellphone in the car after you've car-jacked the car. Now, the problem is that the people who are doing these things are young, male, and in a hurry -- they're going to make mistakes. The police are going to be able to get them. It's just not possible to avoid those kinds of mistakes, especially in a high-stress situation.

Jared Cohen: And of course, our favorite example of the last couple of weeks was I'm sure some of you read about a $45 million ATM heist where literally in a matter of hours, criminals essentially took $45 million out of thousands of ATMs in dozens of countries around the world.

So if you're going to have a partnership between, you know, hackers who are very good at being invisible and transnational organized criminals who are pretty good at staying off the grid. Ultimately they still needed somebody to physically go to the ATM machines and get the money out. And so who did they contract? They contracted street criminals in various places and of various cultures. And what happened in this case? Well, some of the street criminals who maybe weren't necessarily the smartest people in the world, took the money out of the ATM machine and celebrated by posting pictures of themselves with their faces and their cash on Instagram. So thank you anybody who works for Instagram for making that possible…

Eric Schmidt: Well, no-- but come on Jared, but we can do even better. We have John McAfee, right? Our fellow Bay Area resident who managed to move himself to Belize under questioning and suspicion for the death of a neighbor, manages to go on the lamb and he publicizes that he's on the lamb and he's on vacation, he's moving to Latin America. He goes to a hotel in, it turns out, Guatemala. Someone takes his picture and he posts this, showing him in his bathing suit and having a nice time. He was obviously not aware that when you post a photo, it includes your GPS coordinates. Within about one second, someone had taken the metadata of the photo, had figured out where they were. The Guatemalan police show up and arrest him, right -- the good or bad version of the story depending on your point of view. I think the good part of the story is there was no reason to hold him but he was not supposed to be in the country at all, so you get exported back to the United States.

So again, if you're on the lamb, [Laughter] don't -- so remember this: you're on the lamb, turn off the geo-location feature in the metadata as you post pictures of yourself sunning yourself at the beach.

[Laughter]

Greg Dalton: So all the collection availability of this information has given some people concern about sort of big data or the privacy considerations, and I'd like to ask about the Utah Data Center which is being built by the National Security Agency in the United States, reportedly collects 60 billion iPhones worth of data.

That's five zeta bytes? You know what those are, I don't. It's a lot of data. It's going to go online later this year. How should the U.S. approach that? Reportedly, Thomas Drake is an NSA whistle blower who says they will collect information on Americans. Should we be concerned about that much data in the hands of the government given the power of the tools you've been talking about? Eric Schmidt?

Eric Schmidt: We've gone through -- in the industry, we've gone through a series of these proposals, and they're often somewhat over-hyped, in terms of what they can actually do. Let me suggest what can be done. I don't know if this proposal could be done. And then we can debate whether this is a good idea. As I understand it, the NSA's job is essentially foreign communications; they're not allowed to operate in the United States, but I could be wrong there.

Greg Dalton: That's the law, but there's question whether they're actually following that.

Eric Schmidt: Well, if they're not following the law, then somebody will shoot them. That's how it works, right? So --

Greg Dalton: Maybe in some of the countries you've visited in…

Jared Cohen: Maybe they might just arrest them.

Eric Schmidt: That's a joke. Sorry. That's just a joke.

Greg Dalton: You've been spending too much time in North Korea.

Eric Schmidt: That was just a joke. All right. No, come on. You can't ask a theoretical question and then assume that the people are sufficiently incompetent, they're not going to follow the law. So I think we have to assume that any activity is legally appointed. If it's not legal, then people should not do it. Certainly in America. So assuming that this is a legal activity, presumably what they would be doing, and again I'm speculating, is they'd be assembling some of this information and doing data-mining. And the way you would do data-mining is you would look for patterns.

So a simple example is that they're looking for people who are racketeering. Well, you know, you'd look for the signals there. And computers are quite good at tracing this. So far, I've got everybody here in the audience quite upset. Right, you're worried about this, you're worried about your civil liberties. On the other hand, there's some evidence that the surveillance world is actually losing because of the amount of data that's going on.

That in fact, the amount of communication is so overwhelmed the very legitimate and proper functions of the police and the FBI and so forth that in fact we're less safe as a result.

So I'm not going to take a position on the specifics, but I would suggest that when you think about it, think of it in a more nuanced way. Our government does need a certain amount of ability to watch, again, legally and correctly, against in a law and a democracy in a rule of law country like the United States, and the question is there's the proliferation of devices has made it very difficult for them to do it.

Greg Dalton: Jared, your response to people concerned about their civil liberties with all these tools and tracking?

Jared Cohen: There is a way to talk about this at the government level and then just for us as individuals. I think getting nervous about this assumes that different bureaucratic arms of the government are willing and able to work together. So you have -- I'm quite serious. You have different agencies that have different authorities to collect different types of data; they're not so good at working together. And so there's a level of sort of confidence and cohesion that just isn't there. And this is like in a democracy.

So what was interesting is Eric and I went to Mexico to look at how the Mexican government was dealing with the drug cartels, which of course have killed more than 60,000 people in the last five to six years.

We went to see this sort of underground bunker that's called Platform Mexico where they had unbelievable -- I mean you wanna talk about real sort of government cohesion around data related to their citizens, it was here in Mexico. And this is democracy. And so we walked out of this thing thinking, we really hope that no autocracy ever gets their hands on what they built here?

Eric Schmidt: Well, there was more than that. Because you can imagine that, for legitimate reasons, there's a terrible drug war, terrible infiltration of the police, you have to build that in Mexico. So let's assume that they get the problems fixed in five or ten years from now, what are the civil liberties or protections that the Mexican citizens have? Once their systems are built, they're not turned off.

And this, I think, caused us to say, and we indeed say this in the book, that you need to fight for your privacy or you're going to lose it. We were in Britain last week; there was a terrible terrorist act -- one soldier was killed by one apparently lone Muslim extremist in the entire country. And the whole country's excited about this. It's obviously a terrible thing. One person's dead. The home secretary calls for broad regulation and surveillance of the Internet. Not a good thing.

So it's easy for governments to overreact and take away your privacy, your security and so forth in the name of the security. We would say that the open principles, the way in which we work today, is a much, much better way. You'll be ultimately safer with our approach.

Greg Dalton: There's a proposal in California... it’s the right to know measure. It would allow citizens in California to request data from organizations so they could know what companies know about them, and that's similar to what exists in Europe. But the Silicon Valley technology industry has opposed that. Can you tell us about your position on the right to know from consumers? How much information companies have about them?

Eric Schmidt: I don't know the specific legislation so I couldn't comment.

Greg Dalton: It was quite broad and it was -- yeah.

Eric Schmidt: So in general, Google answers this by agreeing with the principle. So you can, for example, in Google there's a panel you can get to where not only will it show what Google knows about you, but you can delete it. And that I think is the correct standard. The general view we have is the information that we collect through our normal course of business with you is really for you to control. And there are some laws that cover that. So for example, we can't just delete all your searches, although we will allow you to do it yourself manually.

But generally, we keep your searches for 12 to 18 months, and that's largely governed by some other

laws. And then we anonymize and get rid of it.

Greg Dalton: Let's quickly ask the audience. How many of you knew that you could delete you could really find out and then delete the information Google knows about you? How many of you -- maybe a third of the audience. A lot of people don't see --

Eric Schmidt: One-third is pretty good. [Crosstalk] no, I think it was a third, Jared.

Jared Cohen: I was rounding up.

Eric Schmidt: But that's not the way to do it. It's a third. Right. So two-thirds have now been educated by the one-third.

Greg Dalton: So Jared Cohen, should people be able to have more access to information that companies hold about them?

Jared Cohen: Well, I think one of the things -- we actually have a whole chapter in the book where we look at the future of privacy and security. And one of the -- there's sort of a broader point that we try to make is, when you look at the existing debate around privacy, it really does center around issues related to this first two billion that are already online. When we traveled around to some of these other environments, as Eric mentioned earlier, you bring up privacy to people and they just sort of look at you like a deer in headlights, like you know, "Who gets privacy?" when you're living in North Korea or Libya or Myanmar.

So we came back with a sense that when you're going to talk about privacy, you need to also talk about security. The two concepts are deeply intertwined. One observation we make is that every generation seems more willing to share than the previous generation. It seems more comfortable with it. Maybe that trend will change. In the book, we make a small argument about the role that parents will play. In the future and on the book tour, we've sort of become champions for the idea that the good old-fashioned methodology of parents intervening and talking to their kids is actually still going to be relevant. And we argue that for -- how many of you, by show of hands, are parents? So a decent amount.

Greg Dalton: About 50 percent.

Eric Schmidt: That would be more than half.

Greg Dalton: More than --

[Laughter]

Jared Cohen: It's like two-thirds.

Eric Schmidt: Two-thirds.

Jared Cohen: So we argue in the book that parents are going to have to talk to their kids about data permanence and online privacy and security years before they have the sex talk with them. It's actually going to be relevant years before that. And by the way, that's not just the case in democracies. Think about a place like Saudi Arabia.

You could imagine a ten-year-old girl, you know, online, active on social networks, saying and doing things that she's not physically mature enough the long-term implications of. And, God forbid, she does something that at the time doesn't carry consequence but, later on in life, follows her around

like a digital scarlet letter with real-world physical implications. Those parents have to talk to that young girl about sort of understanding what the online world means and understand that it's not some parallel universe; it's part of the same world that we already know and what you do and say online has real world consequences.

Greg Dalton: And Eric Schmidt, you think that perhaps at 18, that those ought to be sealed? You talked about 18 --

Eric Schmidt: Well, no. My actually proposal was that at 18, we should have a culture where you just change your name. And you say, "Hey, look. That really wasn't me and so forth." [Laughter] So I actually said this in a conference and it was taken as a serious proposal. It was then and is today a joke. And the reason that it's a joke is that the face recognition is good enough that it won't work.

So, what I like about your questions, Greg, is I think we're getting at the sort of core issue that we want to talk about in the book, which is that there's a set of things that are true about this connected age and the Internet, which brings serious policy questions. The typical example is that companies including Google, through the normal course of business, naturally collect information about that. How do you feel about it? Who should own that? How will it be regulated? How will the companies react? Google's position is largely that you have control over it, but not everyone would agree with that. You could imagine other governments disagreeing with us on that as a principle.

This issue of data permanence means that this generation of children are the first children that are going to grow up with their entire lives completely recorded. I can't imagine what it would be like to have my five-year-old, ten-year-old, fifteen-year-old experiences.

Jared Cohen: We have to talk about the sonograms.

Eric Schmidt: Well, Jared is extremely upset about something.

Jared Cohen: Yeah, the other day I saw somebody posted a sonogram of their unborn child online, and Eric and I --

Eric Schmidt: Without their permission.

Jared Cohen: Because they haven't burped or winked in sort of affirmation that it's okay to do this. And so we argue that not -- it's an illustrative example. Your online identity, in some cases, begins at minus six months or minus five months or whatever a sonogram first emerges.

Eric Schmidt: Jared doesn't have kids yet.

Jared Cohen: But there's actually experts in the audience that can correct.

Eric Schmidt: Look. The fact of the matter is that when -- excluding this sonogram issue, the day you're born, you have a hundred percent control of your identity because you haven't done anything. You've just been born. The birth announcement has just been sent out by your parents. And over your lifetime, the percentage of the control that you have over your own identity declines as a percentage. As you accumulate more and more things people say about you, references, pictures of you with others, crimes you commit, crimes you didn't commit, false charges, and so forth and so on -- all of this is being recorded.

We've never had that situation in any civic society, for everyone to study. It has a lot of implications. A typical example, in America, is that you have a teenager who commits juvenile crime. Let's say it's a modest crime in the scheme of things. They do their time or whatever, their treatment. They

become adults. It's legal in America to get that record expunged if you're good adult. To that point, you apply to a company and there's a little box that says, "Have you ever been convicted of a crime?" And you say, "No, I have never," which you can legally and truthfully do according to the way our legal system works. That person immediately goes on the Internet and sees that you're a liar and, boom, you're out.

How are we going to deal with that? It doesn't seem fair to me, just observing it. That doesn't seem like a good outcome. Maybe the country -- maybe the country's policy was right with respect to teenagers. I think we all understand -- and you say it particularly well, Jared, that the sort of maturity of kids is always going to be behind the world that they're operating in. They're going to continue to make these kinds of mistakes.

Jared Cohen: And also just to add one more thing, because you mentioned crimes, there's a part of the book where we talk extensively about the implications of all of this on people who are incarcerated in prisons. There's a story I heard a number of years ago when I was down in Guatemala. Somebody told me in one of the slums in Guatemala City how they had been repeatedly extorted by somebody who is incarcerated in San Quentin. And so, no matter how secure the prison is --

Eric Schmidt: How?

Jared Cohen: -- they're -- they had a mobile phone.

Eric Schmidt: In San Quentin Prison?

Jared Cohen: So the remarkable thing about prisons is whether you're talking about the most secure prisons in the United States or the least secure prisons in Afghanistan, now for whatever reason, there's just sort of perpetual smuggling problems, and this is unlikely to end. We talk about some of the examples of this in the book. In Colombia, there was a prison where a guy was literally firing SIM cards over the prison wall with a bow and arrow, and it worked for like several months until one of the arrows hit one of the prison guards. [Laughter] Now, that's of course a charming anecdote, but the reason it works is because of the bribery and the amount of resources that these gangs and criminal groups have to pay off the guards.

And so one of the arguments we make in the book is perhaps societies will say if smuggling is a problem that we can't stop and criminals have access inside of prisons, then we shouldn't just incarcerate them physically, we should also incarcerate their online identities.

Greg Dalton: If you're just joining us, our guests today at the Commonwealth Club are Eric Schmidt, Executive Chairman of Google and co-author of "The New Digital Age." We're also joined by Jared Cohen, Director of Google Ideas. I'm Greg Dalton.

We're going to include some audience questions. In fact, we're going to go to a question we received in advance from YouTube. So let's queue that up and then we'll hear this question.

Eric Schmidt: I love using YouTube.

Male Participant: My name is Tobias Enders and I'm from Germany. Currently, I'm an MA student at Hult International Business School in San Francisco. Over the past years, corporate social responsibility has become increasingly important to companies and communities all around the world. I was wondering how Google and other companies in that industry can use their innovations to increase the quality of life for people in emerging markets. For example, for fighting malnutrition or supporting educational initiatives. Thank you.

Greg Dalton: How can Google improve the lives of people in emerging countries?

Eric Schmidt: I like the question because it was submitted on YouTube, obviously. The corporate social responsibility is good for your bottom line because it allows you to get smarter, better employees who feel more empowered and work harder in your company. It's a good business principle as well as a good social principle.

In this particular case, the best thing that I think we've sort of came to is it wiring up the world, which is what's happening now, and accelerating that, is probably the best, if you will, protection for women. It's the best protection against real conflict. It's the best way to avoid some of the problems that have bedeviled the world.

Technically this means the wiring, the connectivity, the applications, getting the price points down. It also, by the way, means getting reliable electric power. Many of these countries have very poor power grids. It means, for example, having telecommunications networks that actually work. Many people in this room are working on this stuff; this is good work.

Jared Cohen: And let me get to the illustrative examples of what Eric is talking about. And the first is in Libya, in sort of the early days of the NATO bombing, Libyan schoolgirls were using Google Maps to plot out where the bombs were falling, so they could find safe passageway to school. And so effective were these maps that the NGOs then started using the information populated by the Libyan schoolgirls to deliver aid. And so you think the Internet matters? It matters a lot for these women in Libya.

Eric Schmidt: Why don't you talk about the Pakistani women…

Jared Cohen: So probably, the most moving experience that Eric and I had on… doing our research for this book and, perhaps, in our entire lives was a trip we took to Pakistan about a year ago.

We met a group of women who had been attacked by the Taliban with acid. And we went to visit them and all of their faces were horribly disfigured. And through no fault of their own, the physical scars that they bear carry a terrible stigma in the physical world that essentially makes it impossible for them to live without sort of being discriminated against or demonized, et cetera. And so when we went to visit all these women, they were all living in a house together. And they all had smart phones, they were learning technical skills, some of them were starting businesses.

And what we realized in talking to them and learning from them is that the Internet had essentially given them a second chance at life because their scars were invisible online. One of them had even met a man online who she developed a relationship with and actually led to them getting married. So do you think the Internet matters? Try talking to a group of women attacked by the Taliban who were given a second chance at life -- it matters a lot.

Greg Dalton: Let's have another question from YouTube for Eric Schmidt and Jared Cohen from Google.

Female Participant: Hi, Eric. I have been very impressed with some of the latest innovation around Google Glasses and self-guiding cars, and wanted to ask you a question around the vision of Google going from software to hardware and the extension of this business model from free advertising services to paid services and devices as well as subscription services. Thanks.

Greg Dalton: So, question about Google's migration… market migration.

Eric Schmidt: I think it's too early to speculate on the exactly this -- the revenue structure.

Obviously, Google Glass at some point is going to get released; we're holding it now working on some of the reasonably obvious privacy issues that people have raised that we expected. The Google Cars, in some form, will be available in years, not decades. Exactly how that will happen we don't really know. We are in the hardware business by virtue of purchasing Motorola.

I use a Motorola phone that's unannounced I particularly like. I think the next round of products for Motorola's going to be fantastic. So I think it'll be first be in these hardware devices, and it may ultimately be some of these other ones as well. It's too early to say.

Greg Dalton: Jared Cohen?

Jared Cohen: The only thing that I'll add is I think it's sort of interesting to see the diversification of the business. I'm obviously newer to Google than Eric is, but one of the things that's extraordinary is how things like driverless cars, things like Google Glass, the ways in which they resonate in parts of the world where people don't even have access to the Internet yet. They literally have never been online, but they're asking us about Google Glass and driverless cars. And so what you learn from all of this, which maybe isn't a perfect answer to your question, is that there's sort of an additional value to all of these connectivity that goes beyond what it does for people who are using it. It's the set of ideas and values that are spread around the world just by virtue of people knowing it's there.

Greg Dalton: And Eric Schmidt, how are you approaching the privacy concerns people have about Google Glass in terms of… Will there be notification? There seem to be quite some concern about that.

Eric Schmidt: I think there's many such answers that we're working on. The issues are obvious: where is it appropriate, where is it inappropriate to be wearing these. There's obviously places where it's inappropriate to be filming and you need to know that. One of the sort of approaches we've taken and try to stay away from the use of face recognition in real-time. That poses a lot of very significant problems, so it's unlikely we will do things in that area.

Greg Dalton: So, you could look at someone and get their identity and --

Eric Schmidt: It could be -- the problem with that is it can be misused.

Greg Dalton: Saturday Night Live did quite a skit on that. That was quite a funny one. We have some questions from Twitter about what are the security implications of the Internet things, botnets and zombies? I'm not sure what that means but --

Eric Schmidt: Botnets are collections of computers that have been harnessed to do a coordinated attack. Zombies are what you'd imagine. They are dead computers that are serving evil purpose and you thought they were dead. They come alive and they do really bad things. So we are at least a colorful industry.

We understand, I think, those problems, and we have technical solutions to them. The biggest threat is not the unknown attacks, but rather the extremely large number of computers that are down-rev. In your company and in your university and in the U.S. government and the state and so forth, there are gazillions of computers that are running down-rev Windows machines. Windows, because it's the number one -- number one, it's the one that's been most attacked by virtue of its simple scale. And so simply upgrading to the latest version of software for those, which is a big task, is probably the single best thing we can do.

For you as individuals, there's a couple of things you should do. The first is obviously you should not

use the same password everywhere. The people who were running the AP Twitter account a couple of weeks ago discovered that. You should not download malware that you don't know about. And people do that, and of course that leads to bad outcomes. And perhaps most important, you should use, by far, the best and most capable browser known as Chrome.

[Laughter]

So if you care about speed, you should use Chrome. If you care about safety, Chrome has never been broken, you should use Chrome. If you care about price, you should use Chrome because it's free. Sorry for the ad.

Greg Dalton: They're all free, I think, right? If you're just joining us, our guests today at the Commonwealth Club are Eric Schmidt and Jared Cohen of Google. Question from the audience: Could you respond to Julian Assange's op-ed in the New York Times? You tweeted about this recently. His charges --

Eric Schmidt: He called us the witch doctors of Google. I've never been called a witch doctor.

Greg Dalton: Is it first? But the point is that -- I mean, underlying was that these technologies actually help totalitarian regimes.

Jared Cohen: Well, first I would start by saying we're not witch doctors. I would also say that in my personal belief, there are some people who, in my view, critique is praise and praise would be critique. That's sort of at a high level how we look at it. But the reality is there are... cat and mouse games have existed between citizens and their governments since the beginning of time. And so you're seeing the same citizen and state dynamic play out in the future as these societies come online. So, then you ask the question "What's changed?" Go back to what I sort of asked all of you in the audience earlier on the session, which is citizens in the future will be able to punch way above their weight and will have a comparative advantage relative to their regimes.

The other thing that I would add is they're going to joined by a whole bunch of transnational meddlers who are altruistic and want to help them. And so in addition to the sort of power of what citizens will be able to do online and by virtue of that offline in their respective societies, a whole new generation of revolutionary helpers will join them.

Eric Schmidt: I think our simplest response is we just disagree. While it's true that the government can organize a surveillance state, the odds of any government including the best run ones, managing to pull that off with the kind of, sort of, the tools and technologies against an informed and empowered populace with mobile phones is highly unlikely to be successful. There's just too many ways in which citizens can get around that. You could imagine a contest between citizens and government in a surveillance state. I know it's romantic to think, "Oh, it's 1984," and all these sort of terrible things are going to happen.

But I don't think the data supports it. I think the data supports that the empowerment of the Internet and mobile phones in particular empowers the citizens at the expense of the state. States should be more worried about it than citizens.

Greg Dalton: We're going to actually over here in this area of the audience Eric wanted to ask some live audience questions, so think over here at the front if you're going to like -- we'll be able to get one or two in after I ask this question. We'll have one or two opportunities for live audience question. This question from Twitter: Given the parallel growth of technology and global greenhouse gas emissions, how can we leverage the new digital age to address climate change?

Eric Schmidt?

Eric Schmidt: That's a very good question. Five years ago here on this stage, we talked a lot about climate change and the opportunities before us. There's a lot of good news to report and there's some bad news. The good news to report is that solar and wind are getting to the point where they're competitive or better than expensive new coal plants, for example. It's a huge win, right. And that's basically because of extraordinary technological improvements in those areas. We have lots and lots of technological improvements in syngas, biofuels, and those sorts of things to give us some hope there.

So there's a lot of reasons to think that the innovation engine is powering much of the U.S. and Europe and so forth can get to where we need to be in renewables. The bad news is that on a rough basis, coal, China is the largest coal emitter. On a gross basis, China is now the largest CO2 producer, and these gaps are just going to get greater. And we, America, are not as efficient on our carbon usage as for example, Germany.

To pull that together, we have more work to do, but ultimately the players are not going to be the U.S. and Europe as much as we wish it were. The players will be the fact that we have an extraordinary large number of people who are coming from basic poverty or very near poverty levels to middle class. And their carbon loading is going to be much higher. The only solution that I can come up with here is to answer with extraordinary needs for additional innovation. The level of efficiency with cars and power generation and so forth, which we celebrate here, if you simply gave all those cars to all of the new people who want cars, you've got an environmental disaster. You've got to get even better. So, from the standpoint of technological -- information technology, which we're talking about, information technology is central to building that innovation network to deliver on this.

Greg Dalton: Does it also require policy? Has President Obama done enough?

Eric Schmidt: This is a problem that governs the globe, and it's not obvious to me how you're going to get the key emitting countries to agree to anything. We've had a series of such initiatives. The president feels very strongly-- I spent a fair amount of time working on this as part of the PCAST-- the president feels very strongly about this. This is a president at the White House that actually believes that climate change is real and that the scientists are correct, shocking, and so spending a little bit of time dealing with the fact that this is a real problem. It affects our children and our grandchildren. This 400 parts per million threshold that we just crossed is something which we're going to regret. And remember that carbon, once added into the environment, does not degrade over thousands of years. So the fact is all you're doing is slowing the rise; and slowing the rise allows generations, five years from now, when we're all dead, to be able to address it.

But we've got a very serious problem here. And so I think we need to talk about it, which is what I'm trying to do. We've got to have innovative policy solutions and we need innovation. It's going to take coordinated action; it's not just the U.S. and Western European problem. The math does not favor -- the current outcome is not good. Just do the math around the developing world. What we saw in our travels was these are people just like us, which means they want the cars and the refrigerators and the lifestyle and the homes and so forth, who are we to deny that from them? We've got to get it to them in a way that's much more efficient carbon-wise.

Greg Dalton: Jared Cohen, you're younger than both Eric and I. You don't have kids yet. How do you think climate change will affect you and your family?

Jared Cohen: Well, I should say that I was very glad that Eric was prepared to answer this question

because it's certainly outside of my area.

I would say one of the things that I've observed is how active the Europeans are on this issue and how much longer they've been active on it, relative to my generation in the U.S. I did my graduate work in the U.K. and I remember going there being surprised that all of my friends just talk incessantly about climate change. I can probably count how many conversations I had with friends about that issue before I went there, and I think we subsequently caught up here in the United States. I think one of the things that started to happen is just much more conversation around it. I think within my generation, there's just sort of the lack of understanding of what the facts are. I think most smart people get that this is an issue, but beyond that, I think there's a lack of clarity on how to break it down.

Eric Schmidt: Greg, you've worked on this for a long time in your career as well. The conversation and knowledge is not the same thing as a solution. I'm very happy that we're having these conversations. I do not see us on a path for a global solution. It is a problem. Call it what it is. We need to address this.

Greg Dalton: Let's get to that audience question. Yes, sir.

Male Participant: Yes, Eric. Andre Broyden. After a massacre in Newtown, there was a lot of search for ways out of this horrific situation when innocent people are shot almost weekly in our country. What I never heard one very simple solution discussed: legal shooting age. So, don't give kids weapons before a certain age and don't teach them to shoot. What do you think about it, Eric?

Eric Schmidt: There's so many guns in America. And by the way, the lobbyists have essentially prevented us from counting them. And even after this terrible massacre, our Congress was unable to enact simple restrictions on gun trading that I'm afraid that any sensible proposal like yours is highly unlikely to get through in the political climate.

And I would ask you rhetorically, how many people have to die from guns that were sold through these trading markets that are not registered? And the problem, by the way, is not legitimate and sane legal gun owners. The problem is that every once in a while, there's a crazy person and they get a gun, too. We have to have this conversation. It's not the sane people. It's the insane people that are killing these people.

Greg Dalton: Let's have one more audience question for Eric Schmidt and Jared Cohen of Google.

Male Participant: Do you think your visit to North Korea, did you have more impact and accomplished more than Dennis Rodman?

[Laughter]

Eric Schmidt: Jared? That's the best question on the entire book tour. Welcome to San Francisco.

Jared Cohen: We should say if Dennis Rodman's advocacy gets Ken Bae out of prison, we will be thrilled that Ken is coming home. It will seriously make us question sort of tactics of diplomacy on what works and what doesn't, which is a whole separate conversation. You know, our visit to North Korea was one of the strangest experiences that Eric and I had ever had. It's really the last frontier in terms of where the Internet is basically absent. When we were there, we came to describe the place as a combination of the movie "The Truman Show" and a Broadway play in the sense that literally everybody we met was an actor.

So Eric had this great idea of, you know, they're not letting us meet any real North Koreans. Let’s go

to the subway and we'll trick them and we'll find real North Koreans. And so we go into the subway and everybody sort of seems polite and diligent. We realize they're all actors. They're literally paid by the government to go back and forth between the only two functioning subway stops and presumably when we leave, they stop commuting and do whatever it is that they do.

So you may ask why did we choose to go there. It was not for a sort of adventure or anything like that. We chose to go there because you have no shortage of governments and diplomats that are making the case to the North Korean regime of what the sort of alternative political path is that they needed to follow. But you have nobody making the technology argument. And what we wanted to do was tell them we wanted to talk about the virtues of a free and open Internet and see if they would let us into the country. And it was not intuitive that they would give us visas, let us into the country and show up at high levels to have that conversation.

We talked to them at lengths, it's not clear whether or not we --

Eric Schmidt: It's worth saying right upfront that there are about a million phones in the country, and they're all perfectly capable of a digital data signal, what is known as a HSDPA signal. And all they have to do is turn it on. It's all they have to do. It's just one decision. And in that country there is one person who can make that decision, and he has not made that decision yet. We certainly hope that they, for lots of reasons involving commerce and pressure from China, we hope that they will empower the Internet in the country. If they do so, they'll become a safer country for us to deal with.

Greg Dalton: We've reached the point where we have time for just one last question, and before we do, I'd like to thank our staff here at the hotel, the Commonwealth Club volunteers, the team at Google has been fantastic to work with. We get to sit up here, but it really takes a lot of people to do that, so I'd like to give them a round of applause, people who have made today possible.

[Applause]

One last question from the audience for Eric Schmidt and Jared Cohen today of Google at the Commonwealth Club. Julia in the audience writes, "How do you recommend that I as a 14-year-old make the most of my high school career while pursuing a future in innovation?" Eric Schmidt?

Eric Schmidt: That is a great question. The first is it's great to be a 14-year-old with the kind of power and tools that are available to you today.

The first thing I would suggest you do is you augment your education with some of the online services. I am partial to something called the Khan Academy. I'm on the board of it and it's a new way of learning and so forth. [Applause] If you are a parent of a teenager or a preteen, I strongly encourage you to use it to supplement their education. It works remarkably well.

Greg Dalton: It's a free online school?

Eric Schmidt: The price is good. It starts with free. So that's the first thing I would do. The second thing I would do is I would use your curiosity. When I was 14, I was infinitely curious about everything, and I hope I still am. So at 14, I'm sure you are and what I would do is I would just spend my time trying to figure stuff out. Every question you have, the things you care about. You'd be amazed at what you can learn. The combination of curiosity and the kind of training you can get on these online things has revolutionized everything. So you can look forward to 80 or 90 years of extraordinary achievements, right, while the rest of us are living off your great work. So thank you very much.

[Applause]

Greg Dalton: Jared Cohen, advice for Julia who's 14?

Jared Cohen: First of all, I love that question for all the obvious reasons. One of the observations that I make about people who are currently teenagers today and generations that will follow them is because technology is so much a part of your life, and because it's been part of your life for such a long time, you don't think of it as an expertise that you have that all the people that you'll work for in the future don't have. So what I would say is whether you go into medicine, whether you become -- you go into academia, whether you go into business, whatever you do in your life, every internship, every job, know that that's your comparative advantage and know that in addition to all the different types of expertise that you develop over the years, you're also going to have that technology expertise. And so, institute your own reverse mentorship program and know that you know more about these tools than everyone you'll work with and you'll do very well.

Eric Schmidt: I think the simple formula is that 14, you start teaching your parents because you know a whole bunch of stuff.

Greg Dalton: Oh, boy. Okay. We have to end it there. Our thanks to Eric Schmidt, Executive Chairman of Google and co-author of "The New Digital Age," [Applause] and Jared Cohen, Director of Google Ideas at Google, also co-author of "The New Digital Age." I'm Greg Dalton. Thank you all for coming in to Commonwealth Club today. Hope to see you again before another five years.

Eric Schmidt: Absolutely.

[END]