Can the Internet of Things be Green and Safe?

https://www.climateone.org/audio/can-internet-things-be-green-and-safe
Recorded on July 20, 2016

Greg Dalton: From the Commonwealth Club of California this is Climate One changing the conversation about America's energy, economy and environment. I'm Greg Dalton. Do you know exactly how much orange juice and butter you have at home right now? Appliance makers are working on smart refrigerators that can scan barcodes of products on the shelves and reorder them automatically. Sixteen years ago Arnold Schwarzenegger had a similar refrigerator in a science fiction movie titled The 6th Day. And consumers could even buy a real one around that time for about $20,000. The movie did pretty well, but the refrigerator flopped.

But today American homes are dotted with Internet connected devices that allow you to manage your home from your smart phone. You can open your front door while you're not there. Adjust your thermostat while driving and spy on your nanny any time anywhere. And there are smart meters that can send power to the grid from solar panels on the roof and EV chargers that can juice up your car overnight when electricity is cheap. On the show today we will discuss what the smart electric grid and Internet of things mean for the American way of life. Is the smart grid vulnerable to hackers and terrorist attacks? Does it endanger your personal privacy? What is the role of the government and private companies in protecting and policing this new frontier?

We're joined by three experts with deep knowledge of these issues. Retired Army General Keith Alexander was head of the National Security Agency from 2005 to 2014 and chief of the U.S. Cyber Command for four of those years. He retired shortly after Edward Snowden leaked documents revealing the NSA was secretly collecting data from all phone calls Americans made inside the country. He's now CEO of a company he founded, IronNet Cybersecurity. Alfred Berkeley served in the U.S. Air Force and was president of the NASDAQ Stock Market from 1996 to 2000. He's been on the boards of WebEx, Safeguard Scientifics and several other companies. He's a director of the World Economic Forum USA and co-author of The New Paradigm for Cyber Security. Dave Mount is partner in the Green Growth Fund of the venture capital firm Kleiner Perkins Caufield & Byers. He's focused on software and services in the energy sector and serves on the boards of UpWind Solutions and Choose Energy. He previously helped manage a portfolio of investments at the oil sector for Sankaty Advisors, a $20 billion unit of Bain capital. Please welcome them to Climate One.

[Applause]

Welcome all of you. General Alexander, this connected world where everything is connected to the Internet. That sounds like a hacker's dream. Is it?

General Keith Alexander: Well, it's a hacker's dream but it's also a dream for us as a nation. When you think about, you know, I was just marveling at this new game Pokémon Go. I don't have it yet. I know my grandchildren, I have 16 grandchildren and they'll say, why not? But when you think about what good is coming out of the Internet. What we, our country created here; there are some phenomenal things that are going on. And just because we're connected doesn't mean we have to forgo civil liberties and privacy. I honestly believe we can do both and should do both. And I think that's part of the discussion I know we'll have today. But it also gets us to a point what can we do with things like renewable energy and tying things to the grid. And some of the Orange Button things that are going on with bringing solar companies together in a more efficient manner to use these energy things for the good of our country. These are tremendous opportunities. So, you know, hackers -- think about numbers, you know, I was thinking about the watching your nanny. I have four daughters and hopefully none are listening right now and they send emails. I don't read all their emails. I'm sorry, my wife does. And I'm a bad father. I have 16 grandchildren I don't read all their emails. So when you think about just the volume of stuff that's going on the practicality of it. And when you think about the numbers, it would take it would be unrealistic.

However, we do need to get the security civil liberty privacy right. And one of the reasons I'm here is we've got to inform the American people about what that means, what's going on and have an informed debate on it. Not one that's sensationalized and inflamed, but one that is informed by the facts.

Greg Dalton: Alfred Berkeley, Silicon Valley, you've been involved with the tech companies. Is this just kind of a, I remember the Segway; some things are going to revolutionize our lives. Didn't happen the way Silicon Valley said it was. How do we know that this is for real, and not just some hype to sell us more gadgets?

Alfred Berkeley: Well it's already changed our lives. We can't economically run this country without connectivity. We have these banking transactions that are going on by the billions, and we don't think a thing of it. And the reason we don't think a thing of it is because they're reliable. They're reliable because they got a lot of smart people trying to make them resilient. And we have benefited from that so much that we don't even notice it.

Greg Dalton: We've surveyed our listeners on Twitter, our followers on Twitter. And we asked them the question; do the greening benefits outweigh the security risks of our ever more connected lives? 60% of the people said that's true, 33% said false and 7% said there are no risks. So our small group on Twitter at least is saying that this is, the benefits outweigh the risk at this point.

I want to roll a clip and then we'll get Dave Mount into the discussion. Samsung and MasterCard have teamed up on a new fridge that can order groceries from a touch screen on the appliance. This is just one example of how the technology business is working on a smart, connected home. Let's listen.

[Playback]

***Male Speaker**: Analysts predict that by 2020, 50 billion things will be connected to the Internet. The equivalent of six devices for every person on the planet. That's the power to transform your home into a connected family hub. Experience seamless ordering from multiple merchants where you can add everyday items to your intelligent card. And pay with a single secure checkout.*

Greg Dalton: So that's a rosy view of an easy life with a smart refrigerator. Now want to hear from another view which is a darker view of how this connected life might play out. And imagine you have a smart house, everything from your lights to your thermostat to your television and water temperature is connected to a smart system. Now imagine that system got hacked and all your devices went haywire at the same time. That's the premise for the season premiere of the TV show Mr. Robot. Let's listen.

[Playback]

Female Speaker*: But what am I supposed to do? Nothing is working. Unplug what? Everything is inside the walls. That's how it was installed when I ordered the smart house package. Now the alarm is going off. And it's freezing, it's below 40.*

Greg Dalton: So that's a woman inside her home with the stereos going on, the alarm is going off. She's talking to someone saying my smart home, everything is going haywire at once. Dave Mount, which of those futures is more likely? Are they both possible?

David Mount: I think that they are both possible and the reality of that second video is something that we should be aware of and that we should plan around and I'll explain that a little bit. So to give a little bit of context around numbers. The Samsung video talks about 50 billion connected endpoints. As we think about the current state of the world, there are say 12, 15 billion connected endpoints today. But in the power sector, in this sector, you know, the energy sector that we're talking about, there are 7,000 power plants in the United States.

So we're talking about going from 7,000 power plants to a world of 50 billion connections or maybe if keeping it in the energy contexts, 7,000 power plants to 200 million solar panels or 120 million air-conditioners in people's homes. And I think that the challenge becomes if each of those control points are potential vulnerabilities for hackers, it is sort of a hacker's dream. I don't think it has to be that way. But I think that the convenience of that connected home case is exciting. But finding ways to make sure that all those controls can't be switched off at the same time is important.

Greg Dalton: Alfred Berkeley, what do you think about that scenario? It is a lot of convenience, but boy, there's a lot of chance. I think back to the days of the flashing clock when people had VCRs or how many people really know how to operate their all the functions on their TV remote control. What do you think about that dystopic or that version of the future?

Alfred Berkeley: Well I think it really gets down to the way people think about resilience. You know, when I buy something I often think about what would happen if I really needed it and it weren't there. I do buy flashlights. I do buy candles. I do buy the things that give me back up. And I think we're going to have to do more of that as things get more connected. But people are smart, they'll figure that out.

Greg Dalton: General Alexander, the smart grid of your company is partly to aim at protecting people or companies from that sort of thing. Do you think that someone could really, you know, mischief, I guess there's a difference between a terrorist attack versus kind of teenagers, you know, wreaking mischief. How do you think that this smart home, you know, could it really go haywire for America?

General Keith Alexander: You know that's exactly what I'm worried about my grandchildren doing to me. It's amazing to see the young people today how wired they are and what they can do with devices. And I think it's a combination of educating, uplifting, informing how do we use these in a safe and reliable manner.

I am more on the first than I am on the second video. I think, you know, yes, people can get in and hack, people can cause problems. We ought to solve that upfront and ensure that the first is the benefit, not the second. So having said that, what it also brings into play is for our nation. What we've had for the last 200 years is we've been secure because of two oceans and hard to get to. And now with the Internet, we're connected to the rest of the world. And so there are two threats to our country, terrorism and cyber. And we can solve those, we've got to solve those and that's, you know, one of the big things that the American people have to step up and say, okay what can we live with, what is the right thing to live with and what do we put forward? And have that debate. And it ought to be a debate in a democracy that puts all that together. Because at the end of the day, we choose, we choose which way we're going to go.

And, you know, it's interesting; I think as Alfred said, there are, we have good people out there. We can solve these issues and I look at how the opportunities for solving cancer, for growing these devices, for connecting; how much you can talk to your family around the world, how you can pass notes. My wife communicates with our daughters, you know, hundreds of miles every day. And it's wonderful and we want that and we can have that.

Greg Dalton: Currently what is the source of the biggest threats? And what's the magnitude of their cyber intervention in the United States? You were head of the U.S. Cyber Command, General.

General Keith Alexander: So I would break the threats out into areas. There's criminal activity that you see going on right now. That's trying to steal money. Why do people steal money in cyberspace? Well it used to be in banks, now it's in cyber. They can steal your identity. They can steal your password and steal money from your bank account. Or they can put ransomware, which will be the biggest one hitting industry today. Ransomware comes in and encrypts all your data and if you want to use it, you have to pay them tens of thousands of dollars and they'll give you a key to decrypt it. That one you're going to see an awful lot about. That's growing, that's the criminal side.

Then you have the theft of intellectual property and that theft of intellectual property really for this area is one of the things that has impacted us most over the last 15 years. We're an innovation nation. There's even books out on this. Look at what goes on in this area, Silicon Valley. You are almost the incubators for ideas for the good of the world for the future. People steal those and then out produce those devices. We lose future capital. That's why I think it's the biggest theft over the years.

And then finally you have nation-states. And when you look at what's going on around the world this is the one that concerns me the most because it has the biggest impact on us as a nation. If things continue to go bad in the Middle East or in Eastern Europe those that wish us harm can most easily do that in cyberspace and we aren't ready. We're making progress, but we're not where we need to be in securing our nation. And that's where government and industry work together for the common defense. And, you know, it's almost back to a point where you look at what our forefathers who made this country when they came up with citizen soldiers, you now are looking at so how do we work together to defend ourselves in cyberspace and what are the ways for it?

So I am concerned about that as a future act, and you saw last month, 14th of June that NATO defense minister said this was a domain of war. And so it's growing it's going to be there. We cannot unilaterally stop it. Those that wish us harm see this is a way to come after us. So we ought to get out in front of it and solve it.

Greg Dalton: And is it nation-states or is it units, you know, there's one building in Shanghai that was part of the Chinese military that was identified, is it nation-states, is it rogue actors, is it these sort of non-state actors, which ones are the biggest threats?

General Keith Alexander: Well for each of those groups and it's interesting. Nation-state actors have the most sophisticated tools and can create the most damage. They're the ones that have the encryption, decryption, all the capabilities that can create significant damage. Some countries allow their people that work day time for these to operate nighttime on the network. So that's a concern, call those your real concern here.

Then you have smart hackers. You can go on-- and I would encourage you to actually get a demonstration and put it out for the people here to see -- of the dark web. Get one of the companies I know IBM and others kinda show what the dark web is and how easy it is to go on the dark web and order malicious software to attack somebody. You can pay $2,000, use bitcoins, get ransomware to go after a company. And when you see that it's they're using the tools that we use for Amazon and eBay to order things to now order like things in the dark web and this is an area of great concern.

So when you look at it I'm worried about the criminal activity, that's the most predominant that's the one if you were to say, I'm going to see a thousand of these and one of these big ones, a thousand of these and one of these. And I think it's that kind of ratio, but these can cause the most significant damage the big attack on it. (0:23:15)

Greg Dalton: If you're just joining us that's General Keith Alexander, former director of the NSA. We're talking about the smart grid Internet of things at Climate One. I'm Greg Dalton. Other guests are Dave Mount, venture capitalist from Silicon Valley and Alfred Berkeley.

Let's talk about some of the celebrated cases. Sony Pictures, Target, the Democratic National Committee all been hacked revealing personal data, corporate data. Dave Mount, what are the lessons of those celebrated hacks?

David Mount: Sure. I think that there are probably three. The first is that typically the way in is pretty unsophisticated. The second may be that the work is once in, it is pretty sophisticated. And I'll start there. So the weigh in on these attacks is typically some sort of phishing. Typically, someone will send an email that they weren't supposed to send. And someone will click a link and click a link that enables a macro in Microsoft Office and then a piece of bad software will get into a computer network. Or in some cases it will be a USB stick; in the case of Stuxnet which is a famous Iranian nuclear case it came in through a USB stick. So typically it's some unsophisticated person on a network that is compromising the intellectual property or in fact, in some case physical assets. So that's unsophisticated first.

The second one and this is maybe a little bit more of a cause for concern for the green grid and the Internet of things is once in, I think the attacks are getting more sophisticated. So this is not necessarily as relevant for Target or the DNC but with Stuxnet with a famous hack that happened in the Ukraine in December, with another hack that has happened-- there have been several hacks in Germany where basically you get into a piece of equipment with a phony email, a phishing email or a USB stick and you can take down multimillion dollar pieces of equipment.

Or in the case of the Ukraine it was takedown 600,000 people's power over the course of a day. And so once in, you're finding people who know how to use sophisticated control systems and know how to use industrial equipment for, you know, pretty powerfully. And there was a German case where a steel mill was actually taken down, the control system was taken over and the mill actually burned itself up. Because someone got in with a phishing scheme and then changed the control system. So I think that those are two of the lessons. I think the third lesson is probably that -- there's a Brandeis quotation. That is, it's something like sunshine is the best disinfectant or sunshine is one of the best disinfectants. And I think it's important in the case of industrial security and the industrial IoT that these hacks become public. And maybe not right away, because there are concerns about making

these vulnerabilities, exposing these vulnerabilities and then allowing them to happen in a sort of cascading way across the world.

But the U.S. government has decided to organize a group that focuses on cyber security in industrials to say look, if we find vulnerabilities, we are going to work with the companies who have those vulnerabilities for -- it's a period of something like 45 days. And if we can fix it in the 45 days, we'll publish a patch. If we can't fix it in those 45 days, we're still going to expose to the world that this is a problem. And I think that they use that, that sort of the concept of sunshine as a disinfectant, to really create some incentive for those companies to do something about it.

Greg Dalton: Alfred Berkeley, is this protecting these things, corporate data, credit card information, shopping at department stores et cetera, is that the job of that corporation, is it the job of the U.S. government? Because cyberspace had been largely free of government intervention; that's why it's so successful.

Alfred Berkeley: Well, I think that as the world gets more integrated and interconnected, there is a role for government. And there's a role for private sector. I spent 11 years working on this public-private partnership issue on a federal advisory committee. And it's very, very difficult because it overlaps with regulation. It overlaps with plaintiffs' bar and lawsuits. It's not a simple issue. That being said, the technology itself is evolving. And one way of looking at what has to happen is that a couple of additional layers to the well-known ISO stack, the description of the way computing works, starting with the chip at the bottom and applications at the top, needs to evolve. There needs to be a structured security layer in there and above at the very top there needs to be structured languages that are being used to describe the information that's coming through the system.

Chips are getting powerful enough now that we're on the verge of being able to get what a password was originally supposed to give you which was security. Passwords were installed way up in that stack I referred to. You're now going to be able to have passwords equivalent much lower in the stack and you're going to be able to have essentially a white labeled Internet where people, where you only deal with people you already know and a blacklisting Internet where you're dealing with the open public. So you're going to get some changes in the technology toward solving these problems, but it's going to take a lot of investment, a lot of cooperation.

Greg Dalton: But General Alexander, isn't for every technological lock, there is a key, there's a way in. And a lot of the tech sector has given up on keeping people out and recognizing people are going to get break your lock however strong it is, is that right?

General Keith Alexander: I'm not sure I agree with that. I think there are ways to secure data. And I think what you have to think about is what's the right standard to go to. Dave mentioned most of the attacks happen because somebody made a mistake. And when you think about what we've asked companies and people who secure networks to do, we're asking them to be right a hundred percent of the time on every area that they're in. And when you think about it, being right a hundred percent of the time having been in the military, you think what's the chances of us being able to count to a hundred, hundred percent. And so you start to look at it and you say okay, somebody is going to make a mistake. And when somebody makes a mistake an adversary gets in.

So what that brings you to is may be the approach were taking doesn't work and we need a new approach. And that new approach may be why don't we have the machines help us secure the things that machines are very good at. What are machines good at? Systematically reviewing everything in an organized way. Going after that, making sure everything is right and they can do it a hundred percent of the time, hundred percent reliable. And let people do what people do really good. We're good at looking at this whole data set. Think about all the information you're taking in right now. As

humans, you're taking in terabits of information visually and not one of you are having a problem doing it. Machines can't keep up with that. And if something happened, you know, a banana came out of one of us all of a sudden you'd notice it right away. So how do we -- well, maybe. And so I didn't take that banana, they're back there we put them back.

But if you think about that, so it really says how do we adjust and evolve our security system. And in my opinion we can do that, we can and must do that. And Alfred brought out about the different layers, so bring all those together. And I think there are some great opportunities coming out that exactly address that. And of course it gets you into so now what you do with respect to security of the system and now security of the nation and how do you provide opportunities for law enforcement and intel community to do the security of the nation while we protect the data the security of individuals.

Greg Dalton: I want to bring this to the grid. Ted Koppel, the journalist from Nightline ABC news wrote a book, Lights Out said that the grid as vulnerable as it is today. And General Alexander, it could be out for a long time. The government is unprepared. He painted a very dark sort of doomsday scenario. How realistic is that?

General Keith Alexander: Well I think what Ted Koppel paints is for a persistent world-class actor that's a threat that we face. And I think what Congress and industry have to do is figure out how do we work together? You bring out an incredibly important point, and that is today as companies and as individuals. If a nation-state were to attack us in cyberspace, should we be expected to be able to defeat a nation-state attacking us? We don't in the physical area. Why is it in cyber and then if we say, no, the government's got to step in there, you get to the question so how do you do that? So the recent cyber legislation was to say, well government and industry ought to be able to pass information back and forth. This is, I can use Sony a little bit better, but it applies to the grid in the Ted Koppel book.

So if you think about Sony being attacked by North Korea, what you want the government to do is not come in after Sony was destroyed and have the government come in and say you lost all your data, you've got everything white. The North Koreans did it, probably did it over a film.

And the people at Sony are going to say well we knew that, that's not helping us. What we really wanted you to do was stop that from happening. When you say, well, that's a good point, but in order for the government to help stop that they've got to see it.

And this is where the air defense picture is a great concept. So think about air defense. Many of you who are going to get on an airplane are really happy that the radars that are down there are going to track your aircraft to make sure your aircraft doesn't hit another one in flight. Bad things happen when that when that occurs, just a technical observation. So if you think about it, what do we do and how do we then bridge the gap with data that doesn't have personally identifiable information industry to government. That's where we've got to get to, so that if it's government that's got to help weigh in they're prepared; or sectors, or individuals, or system. So that's the discussion that I think we've got to have about how we're going to accomplish what Ted. How we going to secure what Ted Koppel puts in his book. And the answer is by working together.

Greg Dalton: Dave Mount, a lot of Silicon Valley companies want the government as far away as possible. And yet, what we just heard from the general is that there needs to be closer collaboration and information sharing with government. What does tech companies think about that?

David Mount: So I think you're right. Most tech companies need to be sure they can succeed without regulation. And that's how they would think about it. If a company requires some piece of

regulation in order to be successful, very difficult to succeed or very difficult to get the backing of venture capitalists. I think in the case of security, and I think, in these discussions that we're having around security for the Internet of things, security for the grid, there is an important distinction to be made around the security of personally identifiable information or emails from a Sony type of situation and the actual physical security that can be at risk because of vulnerabilities around the grid.

And I think that distinction is clear enough where I would say the government probably does have a role in organizing or orchestrating to defend against threats that could have a physical security, safety, impact; some of those things like if a power plant could actually get shut down, the cases that Ted Koppel describes in his book. Those seem disparate and distinct enough from my perspective to warrant having other discussion.

Greg Dalton: General Alexander.

General Keith Alexander: Because I think what Dave said is it very important. And this is where some of you can help. If you think about what's going on right now, you want, everybody here wants to ensure that your bank account is secure. You know, I have $38 in my bank account. I think that's all that's left after the grandchildren. I want that to be secure. And I want my wife's transactions on the web to be secure. I'd like my medical data to be secure. I'd like my communications to be secure with industry and other partners. So you will have one level of security for what we just talked about there.

But my grandchildren who may want to play Pokémon and do all that, they could play we'll call it the Wild West on the Internet. They can have a great time, they can go out there, they can do things and security -- other than I want to make sure that nobody's messing with my grandchildren -- but I think, you know, playing in that area the security issues are far less. So you may have two different areas where you say, yeah, I got to secure the government I'd really like to make sure the power doesn't go out, Ted Koppel saying. I like my healthcare, I like my financial, I put some of these in and some companies are going to say I'd like to be in there too. I'll call that the secure world.

So you have a secure world where everybody comes in and says, I want come in there like I do into the airport. I'll go through TSA, I'll make sure that this aircraft is secure and I'll live by these rules. But in these transactions over here, I want to be in my free world. I can do play, do things and do things over here. I think some kind of evolution there would be in our best interest at least to look at and consider. And I think those are the kinds of things that we have to discuss.

Greg Dalton: General Keith Alexander is the former head of the NSA. We're talking about the green and smart grid at Climate One with other guests, Alfred Berkeley and Dave Mount. I'm Greg Dalton.

We're going to go to our lightning round and ask some brisk questions, single answer questions, starting with Dave Mount. True or false: Alexa the new speech bought from Amazon is more useful than Siri?

David Mount: True.

Greg Dalton: Also for Dave Mount. Alexa sent flowers to your wife for you after a recent argument at home?

David Mount: False.

Greg Dalton: So Alexa can listen and watch everything in your home, right and you don't know exactly what Amazon is listening to?

David Mount: Alexa heard the argument but I was not, I was not smart enough to ask for her to order flowers as well.

Greg Dalton: Alfred Berkeley, the idea of a machine listening and watching everything in your home is a little creepy, yes or no?

Alfred Berkeley: Yes.

Greg Dalton: Keith Alexander, General Alexander, the possibilities of that excites you?

General Keith Alexander: No.

[Laughter]

It actually causes me sleepless nights just thinking about that. No offense to Alfred, I mean.

Greg Dalton: Alfred Berkeley, true or false. Venture capitalists are not as smart as they think they are?

Alfred Berkeley: False.

Greg Dalton: Dave Mount, true or false. Venture capitalists have a terrible track record in the energy sector?

David Mount: True.

Greg Dalton: General Alexander, you enjoy answering questions from guys like me?

General Keith Alexander: Yes.

[Laughter]

Greg Dalton: Alfred Berkeley, the United States has run up huge federal deficits on two wars funded off the national balance sheet and under invested in infrastructure?

Alfred Berkeley: Yes. True, excuse me.

Greg Dalton: Dave Mount, you are glad data stored on your iPhone is encrypted?

David Mount: True.

Greg Dalton: Alfred Berkeley, the NSA can look at it anyway?

Alfred Berkeley: True.

Greg Dalton: General Alexander, your former colleagues peeked at my iPhone in preparation for this program?

General Keith Alexander: False.

[Laughter]

We didn't have your name. We didn't know where you're sitting on it. No, I'm just kidding.

Greg Dalton: Sure. Also for General Alexander you enjoy Jason Bourne movies?

General Keith Alexander: I do. And in fact I look amazingly like him.

[Laughter]

I try to sell that. I know it's not working.

Greg Dalton: They're all the same but they're still good.

General Keith Alexander: He's great.

Greg Dalton: Alfred Berkeley, true or false. Some cyber security companies are hyping the threats of hackers to pump up their business?

Alfred Berkeley: True.

Greg Dalton: Also for Alfred Berkeley, Stuxnet may come back to haunt the United States?

Alfred Berkeley: True.

Greg Dalton: Dave Mount, government protection of data held by companies could be considered a form of corporate welfare?

David Mount: True.

Greg Dalton: General Alexander, the Foreign Intelligence Surveillance Court or FISA court is a rubberstamp?

General Keith Alexander: False.

Greg Dalton: Last one for General Alexander. First word that comes to your mind when I say President Donald Trump overseeing the NSA and CIA.

General Keith Alexander: Wow.

[Laughter]

Greg Dalton: That ends our lightning round. Let's give them a round, thanks them for that.

[Applause]

[CLIMATE ONE MINUTE]

Announcer: And now, here's a Climate One Minute.

The electrical grid of one hundred years ago was fairly straightforward: power went in one end and came out the other – lights on. But with the advent of smart meters, customers have discovered that they can take their household power into their own hands. And as PG&E President Tony Earley tells us, utility companies have also benefited from the technology in ways they didn't expect.

Tony Earley: *But then we discovered, you know, these meters tell us a lot about the system. Back before we had them, we didn't know you were out of electricity unless you called us up. And so if there was an outage at 4:00 in the afternoon because a storm went through we didn't know til you got home and called us. Well we discovered with these meters, we know the meter tells us, "Hey, I'm out!" So we know to mobilize our -- before you even call; in fact we might even get your electricity*

back before you even get home.

Then we found oh we could attach that information coming from the smart meters and we could send it right to our switching gear and if there are a thousand customers out we could switch around so that only the hundred customers nearest where the failure happened are out. And so you can think of this as now the grid is getting smarter and I think we're going to see all kinds of innovations as new technologies come along to be able to make the grid smarter and faster and more efficient.

Announcer: Tony Earley, Chairman and CEO of PG&E. He spoke with Climate One in 2015. Now, back to Greg Dalton and our live audience at the Commonwealth Club.

[END CLIMATE ONE MINUTE]

Greg Dalton: Let's come back to energy. We're talking about a decentralized world where rather than a few small power plants people are making energy, Dave Mount, on their rooftop. How is that better than fossil fuels and is it more vulnerable to attack?

David Mount: Sure. So that decentralized energy picture has a number of benefits. I think it is more sustainable. So there's lower emissions, it's decentralized, it's easier to turn on and off at a small scale. So you can turn it on and off in percentages of a home as opposed to in hundred thousand person increments. So I think that it's safer, it's theoretically more reliable and theoretically safer, theoretically more secure. Can I go into why more secure?

So the theory about the security is the vulnerability of the grid comes at communication nodes. And right now again, there are 7,000 power plants in the United States, each one of them has a generating capacity to serve hundreds of thousands of homes typically. If one of those gets taken out hundreds of thousands of homes go out as well. So the idea is that if you've got millions of solar panels or millions of batteries that are powering people's cars or tens of millions of small micro generators or hundreds of thousands of wind turbines, if one of them fails the consequence of that failure is much smaller. So I think that there is a resilience in a more decentralized grid that has definite benefits.

Greg Dalton: General Alexander, what are the benefits moving away from fossil fuels. You've heard Al Gore give a presentation recently about this. There's a security aspect. So what are the dimensions of moving from fossil fuels to cleaner and what we heard Dave just said more secure energy?

General Keith Alexander: I think it's something that we, the people in this room, our generation should leave for the future generations. When you look at, I was impressed. I saw a presentation from former Vice President Al Gore on climate.

And it was amazing to see the damage that's occurring. And what we can do for solar power and renewable energy to turn that around. We've got to do that. And in doing that, when you think about it where the major power companies like PG&E and others can actually come into play is on creating what Dave was referring to. But I'll take it one step further, a mesh network where solar panels around the country can be used to give a sustainable power with other forms of energy in a way that we've never done before. That's where it's all going to go.

Now the question is do we lead, follow or get out of the way? And, you know, I think what Dixon Wright is doing with Orange Button with Al and trying to push that solar thing is absolutely the right way to go. We are to lead, get small businesses in there help do this. It saves the future for my grandchildren, for our grandchildren. And it's something that we ought to do.

Greg Dalton: General Keith Alexander is former head of the NSA. I'd like to ask Alfred Berkeley, will the incumbent companies the fossil fuel companies, will they try to block and slow down the future the general just described?

Alfred Berkeley: I think there's always a tendency on the part of incumbents to protect what they have. But I think the insurgent newcomers into the game are playing such a forceful game that they're going to force the issue. And you're going to see the existing incumbents trying to get on the sustainable bandwagon.

Greg Dalton: I'd like to talk about your own security. What you do in your life and can suggest to people who have solar panels at home. Dave Mount, you have a very connected life. What do you do to protect your own security and devices and what suggestions would you have to other people?

David Mount: Sure. So in that connected life we do have an Amazon Alexa that we talk to a lot. And my four-year-old son knows how to call up the Star Wars theme song on the Amazon Alexa; it's his favorite thing to do. We have a programmable thermostats. We have a doorbell that has a camera on it. And we have, we live a life that is online. In order to protect that, we do have LifeLock which is a security program that monitors credit agencies to make sure that it knows when personal identifying information is out there. I use two factor authentication everywhere I can, which means when I plug in my password on the website, I typically get a text message from that service confirming that I have my phone with me and putting in a secondary password and I use that. We also use a password manager program that recommends and can sometimes in an automated way change my passwords about once every six months.

So we definitely haven't decided to just kind of put everything online we're doing everything we can to manage the security online. But at the same time we get, I get notes every once in a while from a website that my password may have been compromised and I just view that as the cost of having the benefits of everything else.

Greg Dalton: General Alexander, what kind of passwords do you have and do you use a password manager? I've always thought that that's like putting all the goodies in one place for the hackers to get.

General Keith Alexander: I think what Dave said, I actually do use one. I think LastPass. I think doing that, you know, I want 16 plus character passwords that are really hard to break. And I want, I use LifeLock too and so exactly as you said it. I think those are things to think about for all of us here. And I think LastPass, or companies like that that do this, is actually the wave of the future. I think we will get to biometrics in other ways, but for the time being I think those are the best way and here's why.

If you get all these passwords and you think about all the different things you do, what do you do, you write them down or you put them on your phone or put them in a password file or on a file. Well, shoot, that's just showing somebody where they are. So that's the best thing that I can think of today is using something like that. I think going, I use two factor authentication. So everything Dave said, I do and I think it's great, good job.

Greg Dalton: We're talking about the connected and smart grid at Climate One with you just heard from Alfred Berkeley, director of the World Economic Forum, USA. We also have General Keith Alexander, former director of the National Security Agency and Dave Mount a venture capitalist from Silicon Valley. I'm Greg Dalton.

We're going to our audience questions in a minute. But first I wanted to talk about, get the general

to comment on the Patriot Act where some revisions recently, update us in terms of bulk collection the lone wolf, roving wiretaps. There's some new changes in the Patriot Act I think as of last year.

General Keith Alexander: It's a great question. I'm going to tell this with a story because I think it'll help everybody understand it. You know, you mentioned Snowden. So a year before I left the government, Snowden occurred in 2013, I was called down to the White House for a meeting.

So I go down there and there's this big table, the sit room. You have the National Security Staff on one side, me on the other. I thought, hmm this looks odd. And they say, well we want to have a presidential review group look at NSA and the programs. So they slide these files across the table. And I look up and I'm not going to tell you exactly what I said because I'm not proud of it, but words to this effect, ya-da-ya-da-ya, board member of the ACLU. And I said, you've got to be kidding me. This guy is suing us and you want them to investigate us, that doesn't make sense. Well the president has decided.

So the next day, I go back up to NSA and all these review group guys are coming in. And I'm sitting about where you are, we had big tables. He's sitting there like this. And I thought, body language, all bad. Not yours, but his. And so I say, we're going to tell you everything that we did, we'll be 100% transparent, you'll get to see the whole program. And so I walked them through it and I said, but it won't be the seniors, we're going to let the young people who run these programs over the next five weeks share everything with you. So I and all the seniors left the room and the young people over the next five weeks when the groups came up, ran them through it.

Five weeks later, I come back in the room to see well how did it go. And the guy jumped up from around the table and comes running, I thought he was going to attack me. And I'm in pretty good shape I think I can take him. But he comes running, grabbed my hand and he starts shaking it like this. And he goes you and your people have the greatest integrity of any agency in government. I'm stunned.

And then I said quickly, tell the White House. Tell the American people. Tell Congress and tell the people of NSA. So I'm going to read you something. I had it texted to me while you were asking that question. Just kidding.

[Laughter]

Wouldn't that be good?

Here's what he said publicly, "To say I was skeptical of the NSA is in truth an understatement. I came away from my work on the review group with a view of NSA that I found quite surprising. Not only did I find that the NSA had helped to thwart numerous terrorist plots against the United States and its allies the year since 9/11, but I also found that it's an organization that operates with a high degree of integrity and a deep commitment to the rule of law." Signed, Geoffrey Stone, board member of the ACLU presidential review group member and the acting Dean at the University of Chicago.

Now to get to your specific question, so I get a call last summer. I'm out, and I'm having a great time, you know, I'm doing that. And I get a call from Geoffrey Stone. And he said, the Patriot Act is coming up again. We need to do a joint op-ed. And I think, you're a board member of the ACLU. I'm a former army guy. How could we possibly do this? And he said, it's simple; we should do it for the good of the nation. I thought, okay that makes sense. But why do you want to help push this through? And his answer was simple. He said, if we have another attack we won't have civil liberties and privacy. And this program has the courts, Congress and the administration overviewing it and

we looked at that and wire brushed that, and people looked at that for six months and they've not found one person doing anything wrong that we hadn't asked them to do. (0:53:02)That's what our government needs to do. And I want to support it rather than let something go through that.

So that fall, the Patriot Act was reaffirmed. Now we made two changes and actually, I agreed with both changes with Geoffrey Stone. Keep the data at the service providers and for every time you look at it have a judge say yes, instead of after the fact, before the fact. So that everything that they do, everything that NSA does with that data, everything that they look at and every result is scrubbed by the courts, by the inspector generals in all these areas.

And for the American people, those facts aren't really out there in a way that's digestible. We get the pieces; they're collecting all your data. They're listening to your phone calls or reading your emails. Trust me, you're great people. You're very interesting; nobody is reading your emails from NSA unless you're talking to a terrorist. And then, you want somebody to do that, like the Najibullah Zazi case because that stopped the bombing in New York City that would've killed hundreds of people, stopped by these two programs.

And so from my perspective, we, the American people I'm a citizen soldier now, have got to help set this right. You know, these are good people at the National Security Agency trying to protect us in our way of life. And if Geoffrey Stone, a board member of the ACLU can come out and say, and they're protecting our civil liberties and privacy in doing this in a way that I'm comfortable with, well then, let's help the American people understand that. So Greg, that's where you can help the American people understand it. Because I do think at the end of the day, I joined the Army because I love this country, and I like what we do. And the people that it stood for and the freedoms that we have. And we ought to ensure that. And the military, in the intelligence community that we have out there is doing that.

But they get slammed for the 1% and not credited for the 99% of the good things that they do. And so that's where we've got to set this right. And you asked me a political problem, a question. The reality is we're in the wrong place in politics too if that's where politics are going. You know, this is the greatest country on earth. Made by, you know, I look back at my father in World War II and all those and you think about what these people did to make this country great. Well it's our chance to take the next step and do it with the Internet and do it with what we're doing. And, you know, that's something to be proud of and we oughta all work towards it. I know that took more. I'm sorry. Thank you.

[Applause]

Greg Dalton: We're listening to General Keith Alexander, former head of the NSA. You mentioned Edward Snowden, former U.S. Attorney General Eric Holder joined David Axelrod on his program The Axe Files back in May and weighed in on the debate over Edward Snowden. Let's listen to what he said.

[Playback]

Eric Holder*: We had the capacity to do a whole range of things under these listening programs. But after a while, I remember sending memos to the president asking, you know, do we really need to do this, given the way in which we are focusing on people's lives and given the return that we were getting which was not in any ways substantial. And so I think that, you know, we can certainly argue about the way in which Snowden did what he did, but I think that he actually performed a public service by raising the debate that we engaged in and by the changes that we make.*

Greg Dalton: Former U.S. Attorney General Eric Holder. General Alexander, he said two things that the return was not very substantial. Didn't get security benefit and also that Edward Snowden performed a public service by raising the debate, your response to those two points.

General Keith Alexander: I think that the Attorney General with all due respect is wrong. Here's why. These were not NSA programs. NSA was asked to do these by Congress, the courts and the administration. This isn't something that NSA said geez, let me go do this. And I would just put on one case; I'll give you one case that a true case and you can look it up about what these programs did. And just ask yourselves is that worth it?

In 2009 we intercepted with the 702 the email authorized by the court. If one part was an Al Qaeda related terrorist talking to somebody in the United States, we're authorized to go to one of the service providers, get the email and see what they were saying and if they talk about terrorism, terrorist plots or a terrorist event, to give that to the FBI to protect the country. That connected the dots from 9/11. And we got just such an email on 6th September, 2009. We shared that with the FBI. FBI went and found whose email that was and there was a phone number. And that belong to a guy named Najibullah Zazi. And so three days later they said that phone number that's in there was Najibullah Zazi. By the court we're then authorized to look in the metadata program. And the reason you have it there and you can ask director Bob Mueller and Jim Comey. I said to them, do you need this program, yes or no? And they said, keep it going we need it. And in this case, you are authorized to go one half you see who Najibullah Zazi talking to in one half and then the second half who they were talking to and the third half who they were talking to. In the third half, we saw a terrorist coming back that isolated to a person in New York City. So we were able to say in three or four hours on that phone number that you said was Najibullah Zazi, we see a guy in New York City that looks bad because of this, you ought to go see, we just don't know who it is, we just have a number. (0:59:18)

We don't have a name; we don't have the content on their communications. We have a number daytime group of the calls and that's it. FBI goes and finds a guy in New York City. At that time Najibullah Zazi starts driving across the United States. The email talked about imminent attacks in some place in the United States now believed to be New York City. And the FBI, concerned that the attack was imminent, raided the house of the individual in New York City and found several backpacks with explosives and various states of readiness. That would've been the biggest attack on U.S. soil since 9/11. That would not have happened without these two programs. Hundreds of people in New York City would've been killed. And for me and somebody says well is that worth it? Yes.

Greg Dalton: Let's go to our audience questions. Welcome.

Male Participant: Good afternoon. Thank y'all for your time today. General Alexander, should American companies work proactively with law enforcement agencies or intelligence agencies to provide methods of access for any data collected by IoT devices, even if it's just metadata?

General Keith Alexander: I think companies and the government should work together. I'm not sure I would say proactively. I would say under a framework that we agree with. And here are some of the things that we already agree with.

Child pornography, human trafficking, what about terrorism? And so then the question is, so what is it that we're agreeing to? It goes back to the education question. How much do we want industry to share with government and for what reason? Is it for security or is it for cyber security? On cyber security, we actually want the government to share with industry. Here's all the bad things we're seeing; please give us a heads up. And we want industry to share the same thing with government so we're both protected. And when somebody's getting attacked, we don't have a 911 call. Call 911, get

government help. We are to set up some way of doing that at network speed.

So I think those kinds of things should be set up in a framework that is transparent, that the American people can say I agree with that. And if necessary, have a vote on it. But I think that's a very important point and it gets back to so where and how do you set the framework and where do you set the bar? And that's the debate that we should have.

Greg Dalton: We're coming to the end. I want to bring it back to climate. Earlier, General Alexander framed climate as bit of an intergenerational moral issue. So Alfred Berkeley, what do you think is the most important thing to move away from fossil fuels to get to that clean energy future the general described? What's going to get us there?

Alfred Berkeley: I think that we need in addition to the obvious solar and wind. We need base load hydro. And the technology is coming along to make that work. No dams, free river flow and the power is enormous and it's coming.

Greg Dalton: Dave Mount, you look at lots of different technologies. What's the most exciting to you about moving to that clean energy future to secure the climate get away from fossil fuel?

David Mount: Sure. I have a very exciting vision in my mind of a connected grid that is powered by solar, powered by wind. Taking power into people's homes, powering battery packs and them being used it to power electric vehicles; maybe electric vehicles that drive themselves. And I think that when you have an electric vehicle in your home that becomes a great battery store and sort of takes the intermittency and challenges of what happens when the clouds go over the sky, out of the equation. And I think that -- I hope that seems obvious to us 20 years from now and that that's where we're headed.

Greg Dalton: General Alexander, a lot of the threats we've been talking about hackers or terrorist. They have a face, they're visible and tangible. The climate threat is a little more abstract and it's far away. It's harder for people to see the villain, see the enemy. So how do you suggest making people understand the urgency of climate and then how to get at it?

General Keith Alexander: 2015 was the hottest year in history and before that the hottest year was 2014. Look at the movement and warming of the oceans, the numbers and the strength of the storms that are hitting and the impact on our world. These are life ending events if we don't get our hands around it in 100 years because all the species that we know are either moving to the poles or dying.

And so I think what we're talking about in terms of climate change and what we can do with renewable energies addresses that issue. And again, I think, you know, I'm not political but I was impressed by what former Vice President Gore put out in his program. Now, a fact check on everything could be great; get everything 100% exactly right. But that shows you the issues that we face. And I do think forums like this to use renewable energy and connect them create a super grid, a super smart grid that ties all that together is part of our future and is something that we should welcome.

Greg Dalton: General Keith Alexander is former head of the NSA now head of a cyber security firm. We've also been hearing from Alfred Berkeley and venture capitalist David Mount. I'm Greg Dalton. I'd like to thank our audience here in the room at the Commonwealth Club and online and thank our guests. Thank you all for coming. You can listen to the program at climateone.org and join the conversation on Twitter using our handle @climateone. Thank you all for coming.

[Applause]