AmericanRhetoric.com

Barack Obama

Cybersecurity and Consumer Protection Summit Address

delivered 13 February 2015, Stanford University, Stanford, CA

AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio

First of all, let me thank President Hennessy for not just the introduction but for your outstanding leadership at one of the great universities of the world. I've got to admit, like, I kind of want to go here. I was trying to figure out why it is that a really nice place like this is wasted on young people -- who don't fully appreciate what you got. It's really nice. And everybody here is so friendly and smart, and it's beautiful. And what's there not to like?

I want to thank you and everyone at Stanford for hosting this summit, especially Amy Zegart, George Triantis, and someone who served as a great advisor to me at the White House and as an outstanding ambassador to Russia before coming back to The Farm -- Mike McFaul.

It is great to be here at Leland Stanford Junior University. And I'm pleased to be joined by members of my team who bleed Cardinal red. We're infiltrated with Stanford people. We've got Senior Advisor Valerie Jarrett, National Security Advisor Susan Rice, Secretary of Commerce Penny Pritzker. And, let's face it, I like Stanford grads. I noticed Steve Chu was around here, who helped lead our Energy Department for a while. And he's now hanging out. I'm also pleased to be joined by other members of my Cabinet -- our Secretary of Homeland Security Jeh Johnson is here, and our Small Business Administrator, Maria Contreras-Sweet. And I want to acknowledge my tireless Homeland Security Advisor who helped, and continues to shape, our cybersecurity efforts -- Lisa Monaco. Thank you, Lisa.

So I'd always heard about this campus, and everybody is riding bikes, and people hopping into fountains -- and the current holder of The Axe. This is the place that made "nerd" cool. I was thinking about wearing some black-rimmed glasses, some tape in the middle, but I guess that's not what you do anymore. Ambassador McFaul told me if I came to Stanford, you'd "talk nerdy to me."

But I'm not just here to enjoy myself. As we gather here today, America is seeing incredible progress that we can all be proud of. We just had the best year of job growth since the 1990s. Over the past 59 months, our businesses have created nearly 12 million new jobs, which is the longest streak of private sector job growth on record. And in a hopeful sign for middle-class families, wages are beginning to rise again.

And, meanwhile, we're doing more to prepare our young people for a competitive world. Our high school graduation rate has hit an all-time high. More Americans are finishing college than ever before. Here at Stanford and across the country, we've got the best universities, we've got the best scientists, the best researchers in the world. We've got the most dynamic economy in the world. And no place represents that better than this region. So make no mistake, more than any other nation on Earth, the United States is positioned to lead in the 21st century.

And so much of our economic competitiveness is tied to what brings me here today, and that is America's leadership in the digital economy. It's our ability -- almost unique across the planet -- our ability to innovate and to learn, and to discover, and to create, and build, and do business online, and stretch the boundaries of what's possible. That's what drives us. And so when we had to decide where to have this summit, the decision was easy, because so much of our Information Age began right here, at Stanford.

It was here where two students, Bill Hewlett and Dave Packard, met and then, in a garage not far from here, started a company that eventually built one of the first personal computers, weighing in at 40 pounds. It was from here, in 1968, where a researcher, Douglas Englebart, astonished an audience with two computers, connected "online," and hypertext you could click on with something called a "mouse."

A year later, a computer here received the first message from another computer 350 miles away -- the beginnings of what would become the Internet. And, by the way, it's no secret that many of these innovations built on government-funded research is one of the reasons that if we want to maintain our economic leadership in the world, America has to keep investing in basic research in science and technology. It's absolutely critical.

So here at Stanford, pioneers developed the protocols and architecture of the Internet, DSL, the first webpage in America, innovations for cloud computing. Student projects here became Yahoo and Google. Those were pretty good student projects. Your graduates have gone on to help create and build thousands of companies that have shaped our digital society -- from Cisco to Sun Microsystems, YouTube to Instagram, StubHub, Bonobos.

According to one study, if all the companies traced back to Stanford graduates formed their own nation, you'd be one the largest economies in the world and have a pretty good football team as well.

And today, with your cutting-edge research programs and your new cyber initiatives, you're helping us navigate some of the most complicated cyber challenges that we face as a nation. And that's why we're here. I want to thank all of you who have joined us today -- members of Congress, representatives from the private sector, government, academia, privacy and consumer groups, and especially the students who are here. Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this Information Age.

And it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops. The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security.

Much of our critical infrastructure -- our financial systems, our power grid, health systems -- run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. Foreign governments and criminals are probing these systems every single day. We only have to think of real-life examples -- an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness -- to imagine what a set of systematic cyber attacks might do. So this is also a matter of public safety.

As a nation, we do more business online than ever before -- trillions of dollars a year. And high-tech industries, like those across the Valley, support millions of American jobs. All this gives us an enormous competitive advantage in the global economy. And for that very reason, American companies are being targeted, their trade secrets stolen, intellectual property ripped off. The North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal information of Sony employees. And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security.

As consumers, we do more online than ever before. We manage our bank accounts. We shop. We pay our bills. We handle our medical records. And as a country, one of our greatest resources are the young people who are here today --digitally fearless and unencumbered by convention, and uninterested in old debates. And they're remaking the world every day. But it also means that this problem of how we secure this digital world is only going to increase.

I want more Americans succeeding in our digital world. I want young people like you to unleash the next waves of innovation, and launch the next startups, and give Americans the tools to create new jobs and new businesses, and to expand connectivity in places that we currently can't imagine, to help open up new world and new experiences and empower individuals in ways that would seem unimaginable 10, 15, 20 years ago.

And that's why we're working to connect 99 percent of America's students to high-speed Internet -- because when it comes to educating our children, we can't afford any digital divides. It's why we're helping more communities get across to the next generation of broadband faster, with cheaper Internet, so that students and entrepreneurs and small businesses across America, not just in pockets of America, have the same opportunities to learn and compete as you do here in the Valley. It's why I've come out so strongly and publicly for net neutrality, for an open and free Internet -- because we have to preserve one of the greatest engines for creativity and innovation in human history.

So our connectivity brings extraordinary benefits to our daily lives, but it also brings risks. And when companies get hacked, Americans' personal information, including their financial information, gets stolen. Identity theft can ruin your credit rating and turn your life upside down. In recent breaches, more than 100 million Americans had their personal data compromised, including, in some cases, credit card information. We want our children to go online and explore the world, but we also want them to be safe and not have their privacy violated. So this is a direct threat to the economic security of American families, not just the economy overall, and to the wellbeing of our children, which means we've got to put in place mechanisms to protect them.

So shortly after I took office, before I had gray hair -- I said that these cyber threats were one of the most serious economic national security challenges that we face as a nation, and I made confronting them a priority. And given the complexity of these threats, I believe we have to be guided by some basic principles. So let me share those with you today.

First, this has to be a shared mission. So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.

Second, we have to focus on our unique strengths. Government has many capabilities, but it's not appropriate or even possible for government to secure the computer networks of private businesses. Many of the companies who are here today are cutting-edge, but the private sector doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response across companies and sectors. So we're going to have to be smart and efficient and focus on what each sector does best, and then do it together.

Third, we're going to have to constantly evolve. The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them. Whether it's phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day. So we've got to be just as fast and flexible and nimble in constantly evolving our defenses.

And fourth, and most importantly, in all our work we have to make sure we are protecting the privacy and civil liberty of the American people. And we grapple with these issues in government. We've pursued important reforms to make sure we are respecting peoples' privacy as well as ensuring our national security. And the private sector wrestles with this as well. When consumers share their personal information with companies, they deserve to know that it's going to be protected. When government and industry share information about cyber threats, we've got to do so in a way that safeguards your personal information. When people go online, we shouldn't have to forfeit the basic privacy we're entitled to as Americans.

In recent years, we've worked to put these principles into practice. And as part of our comprehensive strategy, we've boosted our defenses in government, we're sharing more information with the private sector to help those companies defend themselves, we're working with industry to use what we call a Cybersecurity Framework to prevent, respond to, and recover from attacks when they happen.

And, by the way, I recently went to the National Cybersecurity Communications Integration Center, which is part of the Department of Homeland Security, where representatives from government and the private sector monitor cyber threats 24/7. And so defending against cyber threats, just like terrorism or other threats, is one more reason that we are calling on Congress, not to engage in politics -- this is not a Republican or Democratic issue -- but work to make sure that our security is safeguarded and that we fully fund the Department of Homeland Security, because it has great responsibilities in this area.

So we're making progress, and I've recently announced new actions to keep up this momentum. We've called for a single national standard so Americans know within 30 days if your information has been stolen. This month, we'll be proposing legislation that we call a Consumer Privacy Bill of Rights to give Americans some baseline protections, like the right to decide what personal data companies collect from you, and the right to know how companies are using that information. We've proposed the Student Digital Privacy Act, which is modeled on the landmark law here in California -- because today's amazing educational technologies should be used to teach our students and not collect data for marketing to students.

And we've also taken new steps to strengthen our cybersecurity -- proposing new legislation to promote greater information sharing between government and the private sector, including liability protections for companies that share information about cyber threats. Today, I'm once again calling on Congress to come together and get this done.

And this week, we announced the creation of our new Cyber Threat Intelligence Integration Center. Just like we do with terrorist threats, we're going to have a single entity that's analyzing and integrating and quickly sharing intelligence about cyber threats across government so we can act on all those threats even faster.

And today, we're taking an additional step -- which is why there's a desk here. You were wondering, I'm sure. I'm signing a new executive order to promote even more information sharing about cyber threats, both within the private sector and between government and the private sector. And it will encourage more companies and industries to set up organizations -- hubs -- so you can share information with each other. It will call for a common set of standards, including protections for privacy and civil liberties, so that government can share threat information with these hubs more easily. And it can help make it easier for companies to get the classified cybersecurity threat information that they need to protect their companies.

I want to acknowledge, by the way, that the companies who are represented here are stepping up as well. The Cyber Threat Alliance, which includes companies like Palo Alto Networks and Symantec, are going to work with us to share more information under this new executive order. You've got companies from Apple to Intel, from Bank of America to PG&E, who are going to use the Cybersecurity Framework to strengthen their own defenses. As part of our BuySecure Initiative, Visa and MasterCard and American Express and others are going to make their transactions more secure. Nationstar is joining companies that are giving their companies [customers] another weapon to battle identity theft, and that's free access to their credit scores.
And more companies are moving to new, stronger technologies to authenticate user identities, like biometrics -- because it's just too easy for hackers to figure out usernames and passwords, like "password." Or "12345 -- 7." Those are some of my previous passwords. I've changed them since then.

So this summit is an example of what we need more of -- all of us working together to do what none of us can achieve alone. And it is difficult. Some of the challenges I've described today have defied solutions for years. And I want to say very clearly that, as somebody who is a former constitutional law teacher, and somebody who deeply values his privacy and his family's privacy -- although I chose the wrong job for that -- but will be a private citizen again, and cares deeply about this -- I have to tell you that grappling with how government protects the American people from adverse events while, at the same time, making sure that government itself is not abusing its capabilities is hard.

The cyber world is sort of the wild, wild West. And to some degree, we're asked to be the sheriff. When something like Sony happens, people want to know what can government do about this. If information is being shared by terrorists in the cyber world and an attack happens, people want to know are there ways of stopping that from happening.

By necessity, that means government has its own significant capabilities in the cyber world. But then people, rightly, ask, well, what safeguards do we have against government intruding on our own privacy? And it's hard, and it constantly evolves because the technology so often outstrips whatever rules and structures and standards have been put in place, which means that government has to be constantly self-critical and we have to be able to have an open debate about it.

But we're all here today because we know that we're going to have to break through some of these barriers that are holding us back if we are going to continue to thrive in this remarkable new world. We all know what we need to do. We have to build stronger defenses and disrupt more attacks. We have to make cyberspace safer. We have to improve cooperation across the board. And, by the way, this is not just here in America, but internationally -- which also, by the way, makes things complicated because a lot of countries don't necessarily share our investment -- or our commitment to openness, and we have to try to navigate that.

But this should not be an ideological issue. And that's one thing I want to emphasize: This is not a Democratic issue, or a Republican issue. This is not a liberal or conservative issue. Everybody is online, and everybody is vulnerable. The business leaders here want their privacy and their children protected, just like the consumer and privacy advocates here want America to keep leading the world in technology and be safe from attacks. So I'm hopeful that through this forum and the work that we do subsequently, that we're able to generate ideas and best practices, and that the work of this summit can help guide our planning and execution for years to come.

After all, we are just getting started. Think about it. Tim Berners-Lee, from his lab in Switzerland, invented the World Wide Web in 1989, which was only 26 years ago. The great epochs in human history -- the Bronze Age, Iron Age, Agricultural Revolution, Industrial Revolution -- they spanned centuries. We're only 26 years into this Internet Age. We've only scratched the surface. And as I guess they say at Google, "The future is awesome." We haven't even begun to imagine the discoveries and innovations that are going to be unleashed in the decades to come. But we know how we'll get there.

Reflecting on his work in the 1960s on ARPANET, the precursor of the Internet, the late Paul Baran said this: "The process of technological developments is like building a cathedral. Over the course of several hundred years, new people come along and each lays down a block on top of the old foundations, each saying, 'I built the cathedral.' And then comes along an historian who asks, 'Well, who built the cathedral?'" And Baran said, "If you're not careful, you can con yourself into believing that you did the most important part. But the reality is that each contribution has to follow on to previous work. Everything is tied to everything else."

Everything is tied to everything else. The innovations that first appeared on this campus all those decades ago -- that first mouse, that first message -- helped lay a foundation. And in the decades since, on campuses like this, in companies like those that are represented here, new people have come along, each laying down a block, one on top of the other. And when future historians ask who built this Information Age, it won't be any one of us who did the most important part alone. The answer will be, "We all did, as Americans."

And I'm absolutely confident that if we keep at this, if we keep working together in a spirit of collaboration, like all those innovators before us, our work will endure, like a great cathedral, for centuries to come. And that cathedral will not just be about technology, it will be about the values that we've embedded in the architecture of this system. It will be about privacy, and it will be about community. And it will be about connection. What a magnificent cathedral that all of you have helped to build. We want to be a part of that, and we look forward to working with you in the future.

Thank you for your partnership. With that, I'm going to sign this executive order.

Thank you.