**SECRETARY OF STATE HILLARY RODHAM CLINTON**
**REMARKS ON INTERNET FREEDOM**
**TUESDAY, FEBRUARY 15, 2011**

A few minutes after midnight on January 28, the internet went dark across Egypt.

During the previous four days, hundreds of thousands of Egyptians had marched to demand a new government. And around the world—on TVs, lap-tops, cellphones and smart-phones—people followed their every step. Pictures and videos from Egypt flooded the Web. On Facebook and Twitter, journalists posted on-the-spot reports… protestors coordinated their next moves… and citizens of all stripes shared their hopes and fears about this pivotal moment in the history of their country. Millions worldwide answered in real time, "You are not alone. We are with you."

Then the government pulled the plug.

Cell phone service was cut off, TV satellite signals were jammed, and Internet access was blocked for nearly the entire population. The government did not want the people to communicate with each other. It did not want the press to communicate with the public. And it did not want the world to watch.

The events in Egypt recalled another protest movement, 18 months earlier in Iran, when thousands marched after disputed elections. There, protestors also used websites to organize. A video taken by cellphone showed a young woman named Neda killed by a member of the paramilitary forces; within hours, that video was sent around the world. The authorities used technology as well; the Revolutionary Guard stalked members of the green movement by tracking their cellphones. For a time, the government shut down the internet and mobile networks altogether. After the authorities raided homes, attacked university dorms, made mass arrests, tortured, and fired into crowds, the protests ended.

In Egypt, the story ended differently. The protests continued despite the Internet shutdown. People organized marches through flyers and word of mouth, and used dial-up modems and fax machines to communicate with the world. After six days, the government relented, and Egypt came back online. The authorities then sought to use the Internet to control the protests by ordering mobile companies to send out pro-government text messages, and by arresting bloggers and those who organized the protests online. But eventually, 18 days after the protests began, the president resigned.

What happened in Egypt and Iran—where this week again violence was used against protesters—was about a great deal more than the Internet. In each case, people protested because of a deep frustration with the political and economic conditions of their lives. They stood and marched and chanted, and the authorities tracked and blocked and detained them. The Internet did not do any of those things. People did.

But in each country, the ways that both citizens and the authorities used the Internet reflected the power of connection technologies as an accelerant of political, social, and economic change—and in some hands, to slow or extinguish that change.

As a result, there is a debate underway in some circles about whether the Internet is a force for liberation or repression. But that debate is largely beside the point. Egypt isn't inspiring because people communicated using Twitter; it is inspiring because people came together and persisted in demanding a better future. Iran isn't awful because the authorities used Facebook to shadow and capture members of the opposition; it is awful because it is a government that routinely violates the rights of its people.

It is our values that cause these stories to inspire or outrage us—our sense of human dignity, the rights that flow from it, and the principles grounded in it.

And it is these values that ought to drive us to think about the road ahead.

Two billion people are now online—nearly a third of humankind. We hail from every corner of the world, live under every form of government, and subscribe to every system of beliefs. And increasingly, we are turning to the Internet to conduct important aspects of our lives.

The Internet has become the public space of the 21st century—the world's town square, classroom, marketplace, coffee house, and nightclub. We all shape and are shaped by what happens there. All two billion of us and counting.

And that presents a challenge. To maintain an Internet that delivers the greatest possible benefits to the world, we need to have a serious conversation about the principles that guide us. What rules exist—and should not exist—and why; what behaviors should be encouraged and discouraged, and how. The goal is not to tell people how to use the Internet, any more than we ought to tell people how to use any public space, whether it's Tahrir Square or Times Square. The value of these spaces derives from the variety of activities people can pursue in them, from holding a rally to selling their wares to having a private conversation. These spaces provide an open platform—and so does the internet. It does not serve any particular agenda, and it never should. But if people around the world are going to come together every day online and have a safe and productive experience, we need a shared vision to guide us.

One year ago, I offered a starting point for that vision, by calling for a global commitment to Internet freedom—to protect human rights online as we do offline. The rights of individuals to express their views freely, petition their leaders, worship according to their beliefs—these rights are universal, whether they are exercised in a public square or on an individual blog. The freedoms to assemble and associate also apply in cyberspace; in our time, people are as likely to come together to pursue common interests online as in a church or union hall.

Together, the freedoms of expression, assembly, and association online comprise what I have called the freedom to connect. The United States supports this freedom for people everywhere, and we have called on other nations to do the same.

Because we want people to have the chance to exercise this freedom, we also support expanding the number of people who have access to the Internet. And because the Internet must work evenly and reliably for it to have value, we support the multi-stakeholder system that governs the Internet today, which has consistently

kept it up and running through all manner of interruptions across networks, borders, and regions.

In the year since my speech, people worldwide have used the Internet to solve shared problems and expose public corruption—from the people in Russia who tracked wildfires online and organized a volunteer fire-fighting squad… to the children in Syria who used Facebook to reveal abuse by their teachers… to the Internet campaign in China that helps parents find their missing children.

At the same time, the Internet continues to be constricted in myriad ways worldwide. In China, the government censors content and redirects search requests to error pages. In Burma, independent news sites have been taken down with distributed denial of service attacks. In Cuba, the government is trying to create a national InTRAnet, while not allowing their citizens to access the global Internet.

In Vietnam, bloggers who criticize the government are arrested and abused. In Iran, the authorities block opposition and media websites, target social media, and steal identifying information about their own people in order to hunt them down.

These actions reflect a landscape that is complex and combustible, and sure to become more so in the coming years as billions more people connect to the Internet.

So this is a critical moment. The choices we make today will determine what the Internet looks like in the future. Businesses have to choose whether and how to enter markets where Internet freedom is limited. People have to choose how to act online—what information to share and with whom, which ideas to voice and how to voice them. Governments have to choose to live up to commitment to protect free expression, assembly, and association.

For the United States, the choice is clear. On the spectrum of Internet freedom, we place ourselves on the side of openness. We recognize that an open Internet comes with challenges. It calls for ground-rules to protect against wrong-doing and harm. And Internet freedom raises tensions, like all freedoms do. But its benefits are worth it.

Today, I'd like discuss several of the challenges we must confront as we seek to protect and defend a free and open Internet. The United States does not have all the answers. But we are committed to asking the questions… to leading a conversation… and to defending not just universal principles but the interests of our people and our partners.

The first challenge is achieving both **liberty and security**.

Liberty and security are often presented as equal and opposite—the more you have of one, the less you have of the other. In fact, they make each other possible, both online and off. Without security, liberty is fragile. Without liberty, security is oppressive. The challenge is finding the proper measure—enough security to enable our freedoms but not so much, or so little, as to endanger them.

Finding this proper measure for the Internet is critical because the qualities that make the Internet a force for unprecedented progress—its openness, its leveling effect, its reach and speed—also enable wrong-doing on an unprecedented scale. Terrorist and extremist groups use the Internet to recruit members and plot and carry out attacks. Human traffickers use the Internet to find and lure new victims. Child pornographers use the Internet to exploit children. Governments use the Internet to steal intellectual property and sabotage critical infrastructure.

We need successful strategies for dealing with these threats and more, without constricting the openness that is the Internet's greatest attribute.

The United States is aggressively tracking and deterring criminals and terrorists online. We are investing in our nation's cyber-security, both to improve our resilience to cyber incidents and reduce the threat of those incidents. We are cooperating with other countries to fight transnational crime in cyberspace. The United States has led the effort to get multiple resolutions passed at the United Nations, including one this year on cybercrime. The U.S. government invests in helping other nations build their law enforcement capacity. We have also ratified the Budapest Cybercrime Convention, which sets out the steps countries must take to ensure that the Internet is not misused by criminals and terrorists, while still protecting the liberties of our citizens.

In our vigorous effort to prevent attacks or apprehend criminals, we retain a commitment to human rights and fundamental freedoms. The United States is determined to stop terrorism and criminal activity online and offline, and in both spheres we pursue these goals in accordance with our laws and values.

Others have taken a different approach. "Security" is often invoked as a justification for harsh crackdowns on freedom. This tactic is not new to the digital age. But it has new resonance, as the Internet has given governments new capacities for tracking and punishing human rights advocates and political dissidents.

Governments that arrest bloggers, pry into the peaceful activities of their citizens, and limit their access to the Internet may claim to be seeking security. They may even mean it. But they are taking the wrong path. Those who clamp down on Internet freedom may be able to hold back the full expression of their people's yearnings for a while, but not forever.

The second challenge is protecting both **transparency and confidentiality**.

The Internet's strong culture of transparency derives from its power to make information of all kinds available instantly. But in addition to being a public space, the Internet is also a channel for private conversations. For that to continue, there must be protection for confidential communication online.

Think of all the ways in which people and organizations rely on confidential communication to do their jobs. Businesses hold confidential conversations when they're developing new products, to stay ahead of their competitors. Journalists keep the details of some sources confidential, to protect them from retribution.

And governments also rely on confidential communication—online as well as offline. The existence of connection technologies may make it harder to maintain confidentiality, but it does not change the need for it.

Government confidentiality has been a topic of debate during the past few months because of Wikileaks. It's been a false debate in many ways. Fundamentally, the Wikileaks incident began with an act of theft. Government documents were stolen, just the same as if they had been smuggled out in a briefcase.

Some have suggested that this act was justified, because governments have a responsibility to conduct all of their work out in the open, in the full view of their citizens.

I disagree. The United States could neither provide for our citizens' security nor promote the cause of human rights and democracy around the world if we had to make public every step of our most sensitive operations.

Confidential communication gives our government the opportunity to do work that could not be done otherwise. Consider our work with former Soviet states to secure loose nuclear material. By keeping the details confidential, we make it less likely that terrorists will find the nuclear material and steal it.

Or consider the content of the documents that Wikileaks made public. Without commenting on the authenticity of any particular documents, we can observe that many of the cables released by Wikileaks relate to human rights work carried out around the world. Our diplomats closely collaborate with activists, journalists, and citizens to challenge the misdeeds of oppressive governments. It's dangerous work. By publishing the diplomatic cables, Wikileaks exposed people to even greater risk.

For operations like these, confidentiality is essential, especially in the Internet age, when dangerous information can be sent around the world with the click of a keystroke.

Of course, governments also have a duty to be transparent. We govern with the consent of the people, and that consent must be informed to be meaningful. So we must be judicious about when we close off our work to the public and review our standards frequently to make sure they are rigorous. In the United States, we have laws to ensure that the government makes its work open to the people. The Obama Administration has also launched unprecedented initiatives to put government data online, encourage citizen participation, and generally increase the openness of government.

The U.S. government's ability to protect America… to secure the liberties of our people… and to support the rights and freedoms of others around the world depends on maintaining a balance between what's public and what should remain out of the public domain. The scale will always be tipped in favor of openness. But tipping the scale over completely serves no one's interests—and the public's least of all.

Let me be clear. I said that we would have denounced Wikileaks if it had been executed by smuggling papers in a briefcase. The fact that Wikileaks used the Internet is not the reason we criticized it. Wikileaks does not challenge our commitment to Internet freedom.

One final word on this matter. There were reports in the days following the leak that the U.S. government intervened to coerce private companies to deny service to Wikileaks. This is not the case. Some politicians and pundits publicly called for companies to dissociate from Wikileaks, while others criticized them for doing so. Public officials are part of our country's public debates, but there is a line between expressing views and coercing conduct. But any business decisions that

private companies may have taken to enforce their own policies regarding Wikileaks was not at the direction or the suggestion of the Obama Administration.

A third challenge is **protecting free expression while fostering tolerance and civility.**

The Internet is home to every kind of speech. False, offensive, and incendiary speech… innovative, truthful, and beautiful speech. The multitude of opinions and ideas that crowd the Internet is both a result of its openness and a reflection of our human diversity. Online and offline, everyone has a voice. And the Universal Declaration of Human Rights protects the freedom of expression for all.

But we must remember that what we say has consequences. Hateful or defamatory words can inflame hostilities, deepen divisions, and provoke violence. On the Internet, this power is heightened—intolerant speech is often amplified and impossible to retract. Of course, the Internet also provides a unique space for people to bridge their differences and build trust and understanding.

Some take the view that, to encourage tolerance, some hateful ideas must be silenced by the government. We believe that efforts to curb the content of speech rarely succeed—and often become an excuse to violate freedom of expression. Instead, the best answer to offensive speech is more speech. People can and should speak out against intolerance and hatred. By exposing ideas to debate, those with merit tend to be strengthened, while weak and false ideas tend to fade away—perhaps not instantly, but eventually.

This approach does not immediately discredit every hateful idea or convince every bigot to reverse his thinking. But we have determined as a society that it is a far more effective approach than the alternatives. Deleting writing, blocking content, arresting speakers—these actions suppress words, but they do not touch the ideas underneath. They simply drive people with those ideas to the fringes, where their convictions can deepen.

Last summer, Hannah Rosenthal, the U.S. Special Envoy to Monitor and Combat Anti-Semitism, made a trip to Dachau and Auschwitz with a delegation of American imams and Muslim leaders. Many of them had previously denied the Holocaust; none of them had ever denounced Holocaust denial. But by visiting the concentration camps, they displayed a willingness to consider a different view. And the trip had an impact. They prayed together outside the international monument at Dachau and signed messages of peace in the Auschwitz visitors book, many writing in Arabic. And at the end of the trip, they read a statement that they wrote and signed together, condemning without reservation Holocaust denial and all other forms of anti-Semitism.

The marketplace of ideas worked. These leaders were not arrested for their previous stance or ordered to remain silent. Their mosques weren't shut down. The state did not compel them with force; others appealed to them with facts. Their speech was dealt with through the speech of others.

The United States does restrict certain kinds of speech in accordance with the rule of law and our international obligations. We have rules about libel, slander, defamation, and speech that incites imminent violence. But we enforce these rules

transparently. Citizens have the right to appeal how they are applied. And we don't restrict speech even if the majority of people find it offensive. History, after all, is full of examples of ideas that were banned for reasons we now see are wrong. People were punished for denying the divine right of kings, or for suggesting that people should be treated equally regardless of race, sex, or religion. These restrictions might have reflected the dominant view at the time—and variations on these restrictions are still in force in places around the world.

When it comes to online speech, the United States will not depart from our time-tested principles. We urge our people to speak with civility and to recognize the power and the reach that their words can have online. We've seen in our own country how online bullying, for example, can have terrible consequences. Those of us in government should lead by example, in the tone we set and the ideas we champion. But leadership also means empowering people to make their own choices, rather than intervening and taking those choices away.

We protect free speech with the force of law, and we appeal to the force of reason to win out over hate.

**The bet we are making**

The principles I've discussed today are not always easy to advance at once. They raise tensions and pose challenges. But we do not have to choose among them, and we shouldn't. Liberty and security. Transparency and confidentiality. Freedom of expression and tolerance. These make up the foundation of a free, open, and secure Internet—and Internet where universal human rights are respected, and which provides a space for greater progress and prosperity over the long run.

Some countries are trying a different approach—abridging rights online and working to build permanent walls between different activities—economic exchanges, political discussions, religious expression, and social interactions. Their want to keep what they like and suppress what they don't.

But this is no easy task. Search engines connect businesses to new customers, but they also attract users because they deliver and organize news and information from around the world. Social networking sites aren't only places where friends share photos; they also share political views and build support for social causes, or reach out to professional contacts to collaborate on a new business deal.

Walls that divide the Internet—that block political content, ban broad categories of expression, allow certain forms of peaceful assembly but prohibit others, or intimidate people from expressing their ideas—are far easier to erect than they are to maintain. Not just because people find ways around them and through them, but because there isn't an economic internet and a social internet and a political internet—there's just the internet. And maintaining barriers that attempt to change this reality entails a variety of costs—moral, political, and economic. Countries may be able to absorb these costs for a time, but we believe they're unsustainable in the long run.

There are opportunity costs to trying to be open for business but closed to expression—costs to a nation's education system, its political stability, its social mobility, and its economic potential.

When countries curtail Internet freedom, they place limits on their economic future. Young people don't have full access to the conversations and debates happening in the world, or exposure to the kind of free inquiry that spurs people to question old ways of doing things and invent new ones. And barring criticism of officials makes governments more susceptible to corruption, which creates economic

distortions with long-term effects. Freedom of thought and the level playing field made possible by the rule of law are part of what fuel innovation economies.

So it's not surprising that the European-American Business Council, a group of more than 70 companies, made a strong public statement of support last week for internet freedom. If you invest in countries with aggressive censorship and surveillance policies, your website could be shut down without warning, your servers hacked by the government and your designs stolen, or your staff threatened with arrest or expulsion for failing to comply with a politically motivated order. The risks—to your bottom line and to your integrity—will at some point outweigh the potential rewards, especially if there are market opportunities elsewhere.

Now, some have pointed to a few countries, particularly China, appear to stand out as exceptions—places where Internet censorship is high but economic growth is going strong. Clearly, many businesses are willing to endure restrictive Internet policies to gain access to those markets. And in the short term, even in the medium term, those governments may succeed in maintaining a segmented internet. But that doesn't mean those restrictions don't have long-term costs that threaten one day to become a leash that limits growth and development.

There are political costs too. Consider what happened in Tunisia, where online economic activity was an important part of the country's ties with Europe, while online censorship was on par with China and Iran. The effort to divide the economic Internet from the "everything else" Internet in Tunisia could not be sustained. People, especially young people, found ways to use connection technologies to organize and share grievances. This helped fuel a movement that led to revolutionary change.

In Syria, too, the government is trying to negotiate a non-negotiable contradiction: just last week it lifted a ban on Facebook and YouTube for the first time in three years. Yesterday, they convicted a teenage girl of espionage and sentenced her to five years in prison for the political poetry she wrote on her blog. This, too, is unsustainable—the demand for access to platforms of expression cannot be satisfied when using them lands you in prison.

We believe that governments who have erected barriers to internet freedom—whether they're technical filters or censorship regimes or attacks on those who exercise their rights to expression and assembly online—will eventually find themselves boxed in. They'll face a dictator's dilemma, and have to choose between letting the walls fall or paying the price to keep them standing—which means both doubling down on a losing hand by resorting to greater oppression, and enduring the escalating opportunity cost of missing out on the ideas that have been blocked.

Instead, I urge countries everywhere to join us in a bet we have made—a bet that an open Internet will lead to stronger, more prosperous countries.

At its core, it's an extension of the bet that the United States has been making for more than 200 years—that open societies give rise to the most lasting progress; that the rule of law is the firmest foundation for justice and peace; and that innovation thrives where ideas of all kinds are aired and debated.

This isn't a bet on computers or mobile phones. It's a bet on people.

And it's not one that we've made alone. Governments and people around the world have made it too. And we're confident that, together with those partners, by hewing to the universal rights that underpin open societies, we'll preserve the internet as an open space for all. And that will pay dividends for our shared progress and prosperity over the long haul.

**What the U.S. is doing**

The United States will continue to promote an Internet where people's rights are protected and that is open to innovation, is interoperable all over the world, secure enough to hold people's trust, and reliable enough to support their work.

In the past year, we have welcomed the emergence of a global coalition of countries, businesses, civil society groups, and digital activists seeking to advance these goals. We have found strong partners in several governments worldwide. And we have been encouraged by the work of the Global Network Initiative, which brings together companies, academics and NGOs to work together to solve challenges they are facing—like how to handle government requests for censorship or decide whether to sell technologies that could be used to violate rights.

We realize that in order to be meaningful, online freedoms must carry over into real world activism. That's why we are working through our Civil Society 2.0 initiative to connect NGOs and advocates with technology and training that will magnify their impact.

We are also committed to continuing our conversation with people around the world. Last week we launched Twitter feeds in Arabic, and Farsi, adding to the ones we have in French and Spanish. We'll start similar ones in Chinese, Russian and Hindi. This is enabling us to have real-time two-way conversations with people wherever there is a connection that governments do not block.

Our commitment to Internet freedom is a commitment to the rights of people. And we are matching that commitment with action.

Monitoring and responding to threats to Internet freedom has become part of the daily work of our diplomats and development experts, who are working to advance Internet freedom on the ground at our embassies and missions around the world.

The United States continues to help people in oppressive Internet environments get around filters, stay one step ahead of the censors, the hackers, and the thugs who beat them up or imprison them for what they say online. While the rights we seek to protect are clear, the various ways that these rights are violated are increasingly complex. Some have criticized us for not pouring funding into a single technology—but there is no silver bullet in the struggle against Internet repression. There's no "app" for that. And accordingly, we are taking a comprehensive and innovative approach—one that matches our diplomacy with technology, secure distribution networks for tools, and direct support for those on the front lines.

In the last three years we have awarded more than $20 million in competitive grants, through an open process including interagency evaluation by technical and policy experts, to support a burgeoning group of technologists and activists working at the cutting edge of the fight against Internet repression. This year we will award more than $25 million in additional funding. We are taking a venture capital-style approach, supporting a portfolio of technologies, tools, and training, and adapting as more users shift to mobile devices. We have our ear to the ground, talking to digital activists about where they need help, and our diversified approach means we're able to adapt to tackle the range of threats against Internet freedom. We support multiple tools, so if repressive governments figure out how to target one, others are

at the ready. And we invest in the cutting edge because we know that repressive governments are constantly innovating their methods of repression. We need to stay ahead of them.

Likewise, we are leading the push to strengthen cyber-security and online innovation—building capacity in developing countries, championing open and inter-operable standards, and enhancing international cooperation to respond to cyber threats. All this builds on a decade of work to sustain an Internet that is open, secure, and reliable. And in the coming year, the Administration will complete an international strategy for cyberspace, charting the course to continue this work in the future.

This is a foreign policy priority, one that will only increase in importance in the coming years. That's why I created the Office of the Coordinator for Cyber Issues, to enhance our work on cyber-security and other issues and facilitate cooperation across the Department and with other agencies. I have named Christopher Painter, formerly senior director for cyber-security at the National Security Council and a leader in the field for 20 years, to head the new office.

**Conclusion**

The dramatic increase in Internet users during the past 10 years has been remarkable to witness. But that was just the opening act. In the next 20 years, nearly 5 billion people will join the network. It is those users who will decide the future.

So we are playing the long game. Unlike much of what happens online, progress on this front will be measured in years, not seconds. The course we chart today will determine whether those who follow us will get the chance to experience the freedom, security, and prosperity of an open Internet.

As we look ahead, let us remember that Internet freedom isn't about any one particular activity online. It's about ensuring that the Internet remains a space where activities of all kinds can take place—from grand, ground-breaking campaigns to the small, ordinary acts that people engage in every day.

We want to keep the Internet open for the protestor using social media to organize a march in Egypt. The college student emailing her family photos of her semester abroad. The lawyer in Vietnam blogging to expose corruption. The small business owner in Kenya using mobile banking to manage her profits. The philosopher in China reading academic journals for her dissertation. The scientist in Brazil sharing data in real time with colleagues overseas. And the billions of people worldwide who turn to the Internet every day to communicate with loved ones, follow the news, do their jobs, and participate in the debates shaping their world.

Internet freedom is about defending the space in which all these things occur, to ensure that it remains a platform for a vast variety of human interactions. This is one of the great challenges of our time. I hope you will join me in meeting it.

Thank you.