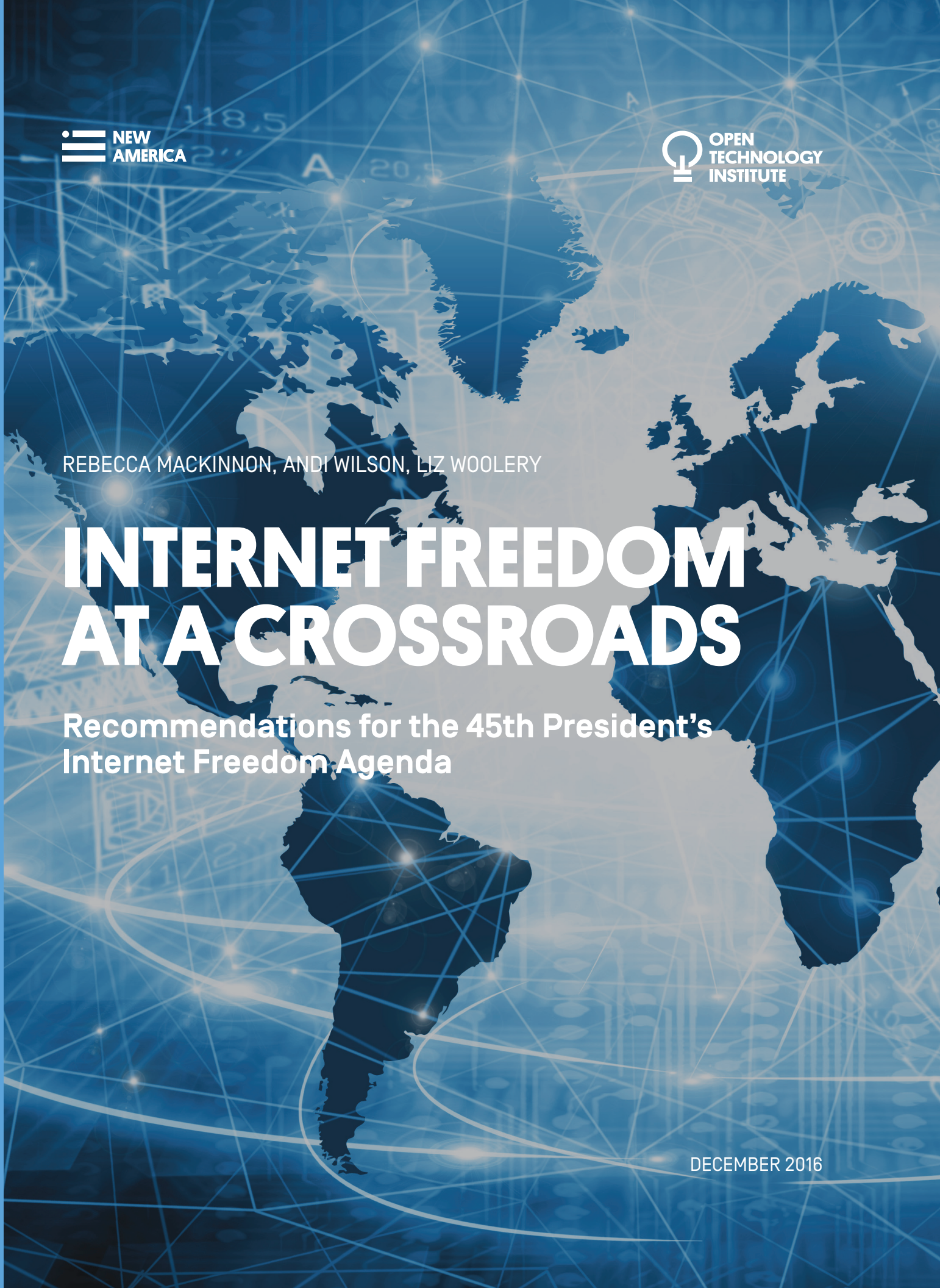

REBECCA MACKINNON, ANDI WILSON, LIZ WOOLERY

INTERNET FREEDOM AT A CROSSROADS

Recommendations for the 45th President's Internet Freedom Agenda

DECEMBER 2016

About the Authors

Rebecca MacKinnon directs the Ranking Digital Rights project at New America, evaluating tech companies on their respect for users' free expression and privacy. MacKinnon is co-founder of the citizen media network Global Voices and author of *Consent of the Networked: The Worldwide Struggle For Internet Freedom*. She was a founding board member of the Global Network Initiative and is currently on the Board of Directors of the Committee to Protect Journalists. Fluent in Mandarin Chinese, MacKinnon was CNN's Bureau Chief and correspondent in China and Japan between 1998-2004. She held fellowships at Harvard's Shorenstein and Berkman Centers, the Open Society Foundations, and Princeton's Center for Information Technology Policy. She received her A.B. magna cum laude from Harvard University and was a Fulbright scholar in Taiwan. She tweets from @rmack.

Andi Wilson is a policy analyst at the Open Technology Institute, where she researches and writes about the relationship between technology and policy. Andi works on issues including vulnerabilities equities, encryption, surveillance, and internet freedom. Before joining OTI, Andi received a Master of Global Affairs degree through the Munk School at the University of Toronto. Andi also worked on political affairs at the Embassy of Canada in Bangkok, Thailand. She tweets from @andiawilson.

Liz Woolery is a senior policy analyst at the Open Technology Institute, where she researches and writes about freedom of expression, privacy, transparency reporting, drones, and internet freedom. Liz is completing her Ph.D. in Mass Communication at the University of North Carolina-Chapel Hill. Liz was the 2014 Google Policy Fellow at OTI and in 2013 interned with the Berkman Center for Internet & Society's Chilling Effects Clearinghouse (now Lumen Database). She received her M.A. in Media Studies from Syracuse University's S.I. Newhouse School of Public Communications and her B.A. from Beloit College. She tweets from @lizwoolery.

Acknowledgments

Internet Freedom at a Crossroads would not have been possible without insight, feedback, and editorial input from Collin Anderson, Kevin Bankston, Daniel Calingaert, Eileen Donahoe, Raman Jit Singh Chima, Bennett Freeman, Robyn Greene, Andrea Hackl, Nathalie Maréchal, Drew Mitnick, Sarah Morris, Eric Null, Courtney Radsch, Ross Schulman, Brett Solomon, Josh Stager, Alison Yost, and the many others who have contributed to this report by offering time, thoughts, and insights, throughout this process. This work has been generously supported by the MacArthur Foundation. The report's authors and New America's Open Technology Institute are solely responsible for the final content.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About OTI

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

INTRODUCTION: A CRITICAL JUNCTURE

A community of Americans who work across the private and nonprofit sectors, who include Democrats, Republicans, Libertarians and Independents, is united in the hope that the administration of President-elect Donald J. Trump will protect, promote, and strengthen freedom online–at home and around the world.

This paper offers a framework for thinking about how the the Trump administration's policies can build on the work of previous Republican and Democratic administrations by continuing to positively support and shape global internet freedom—a policy objective that transcends traditional partisanship. It sets forth a number of recommendations for the next administration's global internet freedom agenda. The goal is not to provide an exhaustive list of everything we would like the next administration to accomplish in relation to internet policy. Rather, it articulates why, how, and on what issues the United States can and should assert leadership.

Support for the promotion of internet freedom cuts across partisan lines for good reason. A free and open internet is not only compatible with the United States' commitment to protect and advance human rights; it is critical to a host of issues that have helped to secure the United States' position as a global leader, including trade and commerce, technological innovation, health, safety, education, and diplomacy.

> **Support for the promotion of internet freedom cuts across partisan lines.**

Today we live our lives online, using the internet to bank, collaborate with colleagues, research health information, share photo albums, take classes, read the news, buy household goods, find jobs, plan for retirement, and so much more. In developing countries, internet access has provided educational materials and medical services previously out of reach. In addition to these day-to-day uses, the internet has played a crucial role in some of the defining moments of the past decade: During the Arab Spring, websites and social media tools helped shape political debate and facilitated protesters' collective activism and dissemination of information as the revolution unfolded.[1] On November 13, 2015, as multiple terrorist attacks hit Paris in a matter of hours, citizens in the area communicated what they were seeing in real time on social media, Facebook's "Safety Check" tool allowed family members to check in with those who worried about them, and

Twitter gave users around the world a platform to share their solidarity with, and send condolences to, those affected by the violence.[2] In the aftermath of natural disasters, political crises, and incidents of terror and violence across the world, the internet has become a vital tool for distributing information and helping people to locate missing family and friends. After Hurricane Sandy, users sent out more than 20 million Tweets about the storm, and New Jersey's largest utility company used Twitter to provide updates on the location of tents and electric generators.[3]

However, despite the promise and power of the internet, freedom online is under threat.[4] We are at a critical moment for the internet. Criminals adapt quickly to new online technologies, deploying them with skill and speed to create new types of threats to individuals, corporations, and governments. Online censorship and surveillance by all types of governments are on the rise. Activists and journalists in a growing range of countries are being jailed for the online publication of facts that are inconvenient for those in power, or for speaking their minds in online news outlets and social media. Encryption, too, has quickly become a matter of worldwide debate. Lack of access to technology remains a problem in poor and rural areas around the world, where greater access to information and ideas could be a powerful tool for change and development.

Government actors continue to endanger and erode human rights online. Authoritarian governments are actively working to erect digital borders to match their physical borders and to prevent citizens from using the internet to hold them accountable through activism, journalism, or peaceful political opposition.[5] Yet internet freedom is also corroded when democratic societies pursue solutions to real and urgent problems such as crime, terrorism, and child protection (among others) without taking into account the full impact of such laws on human rights and internet freedom.[6] Democratically elected legislatures around the world are passing or considering laws whose primary purpose is to advance legitimate law enforcement and national security goals, but do so by prescribing measures that weaken online rights, including privacy and freedom of expression, not only of their own citizens, but of internet users around the world.

At the same time, some powerful commercial lobbies seeking to advance business interests are advocating for policy and regulatory approaches that will, regardless of original intent, make it harder for economically disadvantaged communities to access the internet, preventing billions of people from using new technologies to exercise their rights and take advantage of educational and economic opportunities.[7] Given the challenges democratic societies face in fostering internet freedom at home as well as abroad, the United States is well positioned to play a leadership role in ensuring that global business and trade activities affecting the internet are conducted and regulated in a manner that fosters maximum internet freedom and openness.

Without positive leadership by the world's major democracies, the world's internet users will face further corrosion of their digital freedoms, accompanied by increasingly aggressive attacks by a range of state and non-state actors against the very notion of a free and open global internet, with tangible repercussions in citizens' daily lives.

The United States can lead the democratic world in re-framing the global conversation about security and rights in the internet age. A democratic government is obligated to provide security of life and property for all citizens, not just government and commercial institutions. However, security for citizens is not achievable without the protection of their human rights. This is as true for the online world as for the offline world, even as security challenges for individuals and institutions alike have grown exponentially in their complexity and global interconnectedness in the digital age.

Global internet freedom cannot be maintained—let alone expanded—unless a critical mass of nations commit to internet policymaking approaches built on a clear understanding that security and liberty

are interdependent and symbiotic. It is urgent that all countries—particularly those that claim to be democracies—discard the binary "security versus liberty" frame in pursuing policy solutions that affect citizens' online freedom of expression and privacy.

The Trump administration has an opportunity not only to build on existing frameworks, but also to innovate with new policy approaches that can strengthen global internet freedom. We cannot afford to pass up this opportunity. The goal of bolstering global internet freedom has strong bipartisan support.[8] It is consistent with our global commitments to uphold human rights and the rule of law while also being in the U.S.'s long-term geopolitical and economic interests.[9] The Trump administration can play this leadership role by setting a positive example at home while coordinating a global effort with other nations committed to protecting and promoting a free, open, and secure internet.

PRINCIPLED FRAMEWORK FOR SUCCESS

Four years from now, the success of the Trump administration's internet freedom agenda should be measured by the extent to which the global internet is more open and free than it is today. There should be measurable improvement in the ability of people around the world to use the internet to exercise their political, religious, social, cultural, and economic rights.

In reality, given the many geopolitical forces working directly or indirectly against internet freedom, the stakes could not be higher for all of the people, businesses, and organizations that depend on the internet in order to thrive and prosper.

The Trump administration has an opportunity to assert U.S. leadership by articulating a clear plan and vision for advancing internet freedom in partnership with other like-minded governments, businesses, and civil society organizations around the world.

Core Principles for Internet Freedom

The United States can advance policies at home and abroad that will strengthen global internet freedom by building on three core principles:

Principle 1: Internet freedom starts at home.

The advancement of global internet freedom is undermined if domestic laws and regulations affecting the internet's operation and use are not consistent with international human rights norms, particularly freedom of expression and privacy. The Trump administration has an opportunity to work with stakeholders and elected representatives at all levels and across the political spectrum to build a stronger internet that advances the American people's freedom as well as their security. The administration can also work with stakeholders to establish an impact assessment process to ensure that commercial development and regulation of the internet are both pursued in a manner consistent with the advancement of global internet freedom.

Principle 2: Internet freedom requires effective cross-border policy coordination.

The United States is in a unique position to take the lead in cross-border policy coordination to strengthen global internet freedom. Nations that have committed to the core principles of internet freedom with the support of their citizens—including but not limited to those who have joined the Freedom Online Coalition[10]—should engage in effective policy coordination to ensure that laws governing cross-border platforms and networks, as well as trade agreements and other bilateral or multilateral agreements related to finance, commerce, and security, will be compatible with global internet freedom.

Principle 3: Internet freedom needs accountable multi-stakeholder governance.

The next administration can take concrete steps to advance and strengthen multi-stakeholder internet governance. The first step is to ensure that the institutions and processes that manage internet resources, set technical standards, and coordinate policy are run in a manner that is genuinely accountable, global, and multi-stakeholder. Multi-stakeholder governance and policymaking institutions (the Internet Corporation for Assigned Names and Numbers (ICANN) being the most well known, but not the only such institution) will only be effective if they are sufficiently accountable and transparent to engender trust across a broad set of global stakeholders, including private industry and members of ethnic, religious, political and other groups who face persecution by their own governments. Ensuring that multi-stakeholder internet governance institutions and processes are sufficiently accountable and transparent to maintain global legitimacy will require leadership and innovation on behalf of the United States and other nations committed to a free and open global internet.

> **Four years from now the success of the Trump administration's internet freedom agenda should be measured by the extent to which the global internet is more open and free than it is today.**

KEY CONCEPTS

The terms "internet freedom," "internet governance," and "human rights online" are not always used or understood in the same way. It is therefore important to clarify how the authors of this paper define and understand them.

Internet Freedom

A free and open global internet enables people all over the world to access knowledge, take advantage of educational and economic opportunities, and exercise their fundamental human rights. The State Department describes internet freedom as a policy priority for the United States, with the goal of ensuring "that any child, born anywhere in the world, has access to the global internet as an open platform on which to innovate, learn, organize, and express herself free from undue interference and censorship."[11] This paper builds upon that well-established concept and its related goals which have enjoyed long-standing bipartisan support.[12]

It is important to note that internet freedom does not mean a free-for-all without rules or governance—for the same reason that civil liberties and human rights in the physical world cannot be protected without enforceable laws and accountable governance. Indeed, "internet freedom" as we understand it is not possible without governance.

Internet Governance

In order for information to be exchanged via the internet, technical and policy coordination is required.[13] In 2005 at the UN World Summit on the Information Society (WSIS) during the tenure of then-president George W. Bush, the United States signed on to a working definition of "internet governance" as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[14] This paper builds upon that definition of internet governance, around which there continues to be strong bipartisan consensus.

Due to the internet's globally interconnected nature, actions that one government or polity takes to regulate the internet in one jurisdiction can affect internet users all over the world. When one legislature passes a law affecting what companies or people can do in relation to the internet (for example, a law requiring companies to monitor users for copyright violations, or a law requiring companies to handle user data in particular ways), that law affects people and entities in other countries and regions. Those people did not vote for the lawmakers who passed that particular law; their concerns or interests were

likely not considered. Nonetheless, such affected individuals, organizations, companies and even other governments all have a stake in internet governance—in other words, they are stakeholders. Even when a law seeks to address an internet-related problem that is local in nature, stakeholders across the world tend to be affected in some way, regardless of whether the law's authors ever took them into consideration.

New approaches to governance have evolved along with the internet itself. Technical standards that enable the internet to operate globally, initially developed by engineers in universities and companies, are coordinated primarily by "multi-stakeholder" governance bodies including ICANN. While such institutions continue to evolve and critics question their accountability, their authority is based on the recognition that internet policy solutions achieved through multilateral agreements via conventional politics and geopolitics are not fit for purpose and cannot achieve adequate legitimacy among the many stakeholders whose buy-in is required if governance is to be successful.

Human Rights Online

The United States was a key driver of a 2012 UN Human Rights Council resolution asserting that human rights in the physical world extend fully to the online world.[15] These rights, as articulated by the Universal Declaration of Human Rights (UDHR)[16] and other international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR)[17], include the rights to freedom of expression (Article 19 of the UDHR and ICCPR) and privacy (Article 12 of the UDHR and Article 17 of the ICCPR), as well as the other rights including peaceful assembly, political association, property ownership, education, freedom of thought and religion, etc. A key function of governance is to create the conditions for the enjoyment and protection of rights, as well as mediation between conflicting rights, which necessarily means the setting and enforcement of rules. Limitations on one person's rights in order to protect another's must meet certain conditions, however, they must have a legal basis and be carried out in a transparent and predictable manner. Limitations must also be "necessary and proportionate"—necessary to protect life and the rights of others, and proportionate by using the least-restrictive means to achieve the objective.[18]

Even when a law seeks to address an internet-related problem that is local in nature, stakeholders across the world tend to be affected in some way, regardless of whether the law's authors ever took them into consideration.

In 2011, the United States supported the UN General Assembly's endorsement of the UN Guiding Principles for Business and Human Rights, which affirm that states have the primary duty to protect human rights while business enterprises are responsible for respecting human rights.[19] In order to be compatible with international human rights norms, any governance processes or mechanisms must foster the ability of nation-states of protecting human rights, and the ability of private actors to respect human rights, regardless of whether governance is conducted through the more traditional political and governmental systems of nation states, or through newer international and/or multi-stakeholder governance mechanisms. Given the private sector's role in the creation and functioning of the internet, the human rights obligations of non-state actors as well as state actors cannot be understated. In the long run, only an internet governance regime based on a clear commitment to international human rights principles can gain global legitimacy, and thereby succeed in maintaining a free and open global internet.

U.S. LEADERSHIP OPPORTUNITIES FOR FOSTERING GLOBAL INTERNET FREEDOM

A Guide to Our Recommendations

Building on the principles and definitions articulated above, we have identified several opportunities for U.S. leadership in the advancement of global internet freedom. These opportunities are organized under three broad headings:

1. **Free Flow of Information**: The U.S. can lead in tackling some of the most challenging policy problems that have arisen over the past decade related to internet access and online content in a manner that bolsters freedom of expression across the globe.

2. **People-Centric Security**: The U.S. can lead in building consensus among nations committed to a free and open internet around new policy approaches to privacy and security that recognize the interdependence between security and human rights, including freedom of expression and privacy.

3. **Accountable Multi-Stakeholder Governance**: The U.S. can play a leading role in strengthening multi-stakeholder internet governance institutions.

In compiling the recommendations below we have not attempted to make an exhaustive catalogue of all issues related to internet freedom that we believe the next administration must work on. Rather, we have focused on areas where United States not only can—but must—assert stronger global leadership.

1. Free Flow of Information

Efforts to support the global fight against authoritarian internet censorship started under the George W. Bush administration, then were continued and expanded throughout the Obama administration. In 2011, the U.S. partnered with a group of governments committed to advancing global internet freedom to found the Freedom Online Coalition (FOC), whose membership has doubled in size from 15 to 30 countries over the past five years.[20] Yet censorship around the world has continued to grow in scope and complexity over the past decade. Freedom House recently reported the sixth straight year of decline in global internet

freedom since the organization launched its annual Freedom On the Net report in 2010.[21]

The free flow of information online is vulnerable at many levels: At the most basic level, internet freedom cannot be enjoyed by those who, due to geography or economics or both, have little or no access to the infrastructure needed to connect to the internet. When people do have internet access, access to content and communications can be thwarted by government-imposed internet shutdowns, cyber-attacks that cripple or bring down networks, or by the filtering or blocking of specific services or content. Even if blocking or shutdowns do not occur, content and communications—including social media and mobile messaging services—can be restricted or blocked by the internet backbone operators or the content platforms and communications services themselves. The U.S. is in a unique position to champion the free flow of information at all three levels.

✓ ***Champion access to networks and services***

Government-sanctioned shutdowns, interference, and disruptions of network connectivity are the most direct form of censorship and pose a significant threat to freedom of expression around the world. **The Trump administration can lead the advancement of internet freedom by engaging on a global scale to end the practice of government-led network shutdowns.**

Unfortunately, such obstructions to internet access are commonplace in a number of countries and have even become the norm for some governments seeking to control or crackdown on access to and dissemination of information.[22] In the first half of 2016, there were more than 20 internet shutdowns across the globe, taking place in Algeria, Brazil, Syria, Turkey, and Vietnam, among other countries.[23] While limiting or completely cutting off access to the internet anywhere is detrimental to human rights, in countries rife with conflict and war, where shutdowns are increasingly common, the effect is all the more problematic.[24] Citizens of those countries have access to few accountability or "watchdog" resources and limited exposure to potential sources of aid or help.

Importantly, internet shutdowns can be specific, targeted, and strategic. Shutdowns can occur at various levels of access, such as prohibiting access at a national or regional level, prohibiting access to specific domains, or prohibiting access by specific IP addresses.[25] Further, shutdowns are often be responsive to certain political situations. Previous service disruptions have targeted those individuals, such as journalists and activists, whose communication with the outside world is most threatening to the reigning power. In addition, by their very nature, shutdowns (much like filtering or blocking content) interfere with the ability to communicate, gain access to information, or disseminate information, all of which are critical during times of conflict, war, and protest.

The United States has a key role to play in ensuring that states stop the practice of engaging in internet shutdowns. One approach to tackling the problem of network shutdowns may be to leverage existing memberships in multi-stakeholder and multilateral organizations in order to to fight internet shutdowns. As part of this effort, the United States can work with other members of the FOC to press authoritarian regimes to end censorship and treat internet access as a fundamental human right.

✓ ***Champion the growth and strengthening of internet infrastructure***

Another component integral to the free flow of information is the infrastructure through which communications are shared and accessed. Inadequate or non-existent physical infrastructure severely limits access to the internet, including critical cultural, educational, and medical resources. Often, those most in need of access to these online resources are the most likely to lack sufficient (if any) access to the internet.[26] While resolving issues of access to the internet requires a multifaceted approach, the physical infrastructure underpins any and all potential approaches. **The United States has a historic opportunity to lead**

by example, strengthening domestic internet infrastructure as it supports efforts to bridge digital divides around the world.

The Trump administration should work to remove barriers to competition so that disruptive models can flourish. The United States tends to lag behind global peers in terms of both speed and cost of broadband access. The exception is in those places where there are new or disruptive models, such as Google Fiber or municipal networks, in place. These networks lower the cost of internet access, in turn mitigating a frequently-identified barrier to broadband access in low-adoption communities. Unfortunately, roughly 20 states have laws that limit or entirely ban deployment of municipal broadband networks.[27] The next presidential administration can encourage states to remove these barriers to municipal networks and public-private partnerships that can grow and strengthen broadband networks. Similarly, communities should be encouraged to explore public or public-private models for networking. A push to empower state and local governments will be a key aspect of allowing new internet service models to flourish and serve as an example to communities abroad.

Prioritize infrastructure investments in order to increase access to broadband. Recent presidential administrations have focused on growing and improving these physical networks and connections that facilitate access to the internet. One approach to this was undertaken with the Broadband Technology Opportunities Program (BTOP), signed into law by President Barack Obama as part of the American Recovery and Reinvestment Act of 2009.[28] Through a series of competitive grants, BTOP funding has been used to construct or upgrade roughly 120,000 miles of broadband networks across the country.[29] Nearly two decades (and three presidents) before BTOP began, Congress signed the High Performance Computing Act of 1991 (also known as the "Gore Bill," after then-Senator Al Gore) into law. The act led to creation of the National Information Infrastructure and spurred development of NCSA Mosaic, "the first web browser to achieve popularity among the general public,"[30] which in turn shaped how future generations would interact with the World Wide Web. When then-President George H.W. Bush signed the act into law, he pointed to the act as a demonstration of the United States' leadership in information technology development[31] and hailed the act as having "the potential to transform radically the way in which all Americans will work, learn, and communicate in the future."[32]

> **A national dig-once policy is an easy, bipartisan action that would move the United States toward greater broadband saturation and ensure that more citizens can access critical online resources.**

This administration can also promote a national "dig-once" policy and encourage other countries to do the same. Deemed a "no-brainer" by the *Washington Post*,[33] dig-once policies are designed to curb repeat disruptions of federally funded highway construction projects when such disruptions are the result of growing demand for installation of conduit lines, cables, and other infrastructure necessary for broadband access. The most expensive part of broadband deployment is the burying of cables and conduit lines.[34] A dig-once policy would both alleviate some of that cost and, at the same time, expand broadband offerings. Dig-once policies emphasize coordination between government agencies and utility companies in order to minimize the amount and frequency of excavation required to install the infrastructure necessary to deploy networking conduits.[35] Several states, including Arizona, Minnesota, and Utah, as well as municipalities, including San Francisco and Boston, have implemented these policies as part of efforts to save money, time, and increase access to the internet.[36] A national dig-once policy is an easy, bipartisan action that would move the United States toward greater broadband saturation and

ensure that more citizens can access critical online resources.

Strengthen and support the Global Connect Initiative. If the United States can lead by example as described above, the next administration will be in a stronger position to lead international efforts to expand and strengthen the necessary infrastructure to bring the internet to those who currently have no access. Launched in September 2015 by the State Department, the Global Connect Initiative (GCI) aims to bring 1.5 billion people online by 2020.[37] The program's implementation relies on a global group of supporters drawn from a diverse mix of governments, trade groups, major corporations, development banks, and civil society organizations.[38] Those supporters agree to adhere to the Initiative's principles, including integrating internet connectivity into national development planning, fostering digital literacy, and creating environments that are conducive to the innovation required to reach universal connectivity.[39] GCI's roadmap for implementation dovetails nicely with the other recommendations here, including support for integrating dig-once policies into infrastructure practices.[40]

To date, the U.S. has convened supporters to identify projects and policies that contribute toward GCI's goal. The roadmap for GCI focuses on regular convenings that offer opportunities for the diverse group of supporters to hear about new initiatives, follow up on existing ones, and maintain momentum while pushing for 1.5 billion more internet users by 2020.[41] As this initiative has been spearheaded by the U.S. government, it falls on the next administration to continue to back the Global Connect Initiative by committing to the necessary policy, financial, staffing, and other forms of support.

A key challenge for Global Connect is not merely connecting people—but connecting them to networks through which people can exercise their rights to freedom of expression and assembly, and where their right to privacy is respected and protected.[42] Thus the Trump administration can exert global leadership by working with other governments, the private sector, technical experts, and civil society to ensure that as infrastructure for connectivity is strengthened and extended around the world, the internet services made available to the world's next billion internet users are operated in a manner compatible with internet freedom.[43] Governments, international organizations, and private entities contributing financially to Global Connect should work with recipient countries and private sector partners to ensure maximum transparency and accountability around the way in which information is controlled and governed through this new infrastructure.[44]

The Trump administration has an opportunity to advance related goals by **supporting timely Senate passage of the Digital GAP Act**, which passed the House with strong bipartisan support in September 2016.[45] The bill would enshrine "dig once" as an official element of U.S. development strategy in funding or facilitating international internet infrastructure projects around the world. It would also require greater transparency in U.S.-supported infrastructure projects.[46] Improved transparency would make it easier for the private sector to coordinate private infrastructure investments with official efforts, and for other stakeholders including civil society to engage with them to ensure that they are compatible with internet freedom principles.

✓ *Champion freedom of expression on content and communications platforms*

A decade ago, wholesale blocking or "filtering" of websites was the preferred method of government internet censorship, carried out mainly by authoritarian regimes.[47] Since then, many governments have shifted the focus of their censorship to the platforms that host content, such as web hosts, social media companies, and chat applications. In 2010, "intermediary censorship," whereby governments demand that companies hosting content and social media remove specified postings, delete entire pages or sites, or deactivate user accounts, was identified by researchers as a new practice pioneered in China.[48] By 2015, Freedom

House reported a dramatic growth in the number of countries that "required private companies or internet users to restrict or delete web content dealing with political, religious, or social issues."[49] Companies like Google, Facebook, and Twitter have documented in their regular transparency reports a steady rise in government demands to remove content and deactivate accounts from all kinds of countries, including many democracies.[50] Intermediary censorship is now a fully global phenomenon.

At the same time, it is an inescapable fact that online harassment, hate speech, and extremist content pose genuine threats to civil discourse as well as many people's physical safety. International human rights law provides for the restriction of content which itself threatens people's ability to exercise their own rights to expression, belief, and assembly or even enjoy a basic right to security.[51] In order to prevent the abuse of power and overbroad censorship any measures to restrict speech should be necessary (i.e., using the least restrictive means to achieve the objective), proportionate, and based in law.[52]

The constitutional and legal frameworks of most democracies allow for the sanctioning and censorship, to varying extents, of a range of threatening and defamatory speech that is constitutionally protected in the United States.[53] It is primarily for this reason that companies like Facebook, Google, and Twitter have in recent years documented large numbers of requests to remove content or restrict accounts made by authorities in democratic countries like Brazil, India, Germany, and France.[54] More repressive regimes outlaw even wider ranges of content under much more broad and often vague justifications of incitement, defamation, blasphemy, and terrorism, charges which result in the censorship and arrest of journalists and activists.[55]

However, in the United States, the First Amendment protects speech that may be hateful, speech that is untrue, and speech that is critical of public officials. At the same time, companies are free to police their own privately owned and operated platforms as they see fit, through the use of rules commonly known as "terms of service" to which users are required to agree if they want to use the service.

It is against this backdrop that companies face increasing pressure at home and abroad to fight violent extremism on global social media platforms. Silicon Valley has responded to pressure, criticism, and appeals to patriotism from Congress and various parts of the executive branch by amending their terms of service and strengthening enforcement measures against a wide range of content that advocates or is associated with violent extremism.[56] In Europe where governments lack the same constitutional constraints against direct action, the European Union has all but compelled companies to sign on to a code of conduct, pledging to take stronger action against "illegal hate speech."[57] Government-sanctioned efforts to work with companies to remove terrorist-related material, such as the United Kingdom's Counter Terrorism Internet Referral Unit (CTIRU),[58] have faced challenges differentiating between content that is in fact glorifying or selling terrorism versus content that is shared in the context of online debate, or information that is newsworthy, or even advocating against terrorism. When the distinctions are not correctly made, internet users' rights are violated

Freedom House reported a dramatic growth in the number of countries that "required private companies or internet users to restrict or delete web content dealing with political, religious, or social issues."

and the resulting "collateral" censorship corrodes internet freedom. Human rights groups and activists have documented numerous examples in which journalists, activists, and even innocent bystanders (such as women named "Isis") have been victims of such collateral censorship.[59]

The United States, as the home of the world's most popular and powerful social media platforms, is in a unique position to ensure that efforts to counter violent extremism online do not undermine internet freedom.

The concern is not that companies are cracking down on violent extremism per se, but rather that measures are being taken without clarity of scope or definition regarding what constitutes "extremist" speech and who decides.[60] Neither the companies' beefing up of terms of service, nor the EU code of conduct with companies involved consultation with human rights groups or independent technical experts. No human rights risk assessments have been carried out and mechanisms for appeals or redress have not been strengthened in parallel with the strengthened rules and enforcement. When the White House held a meeting with Silicon Valley executives in early 2016 to discuss how to fight online extremism, civil liberties, and human rights groups were not invited.[61] In response to those communities' concerns, the White House ultimately also consulted with several groups, including New America, regarding its initiatives to counter violent extremists, consultation that should continue under the Trump administration.

As the United States develops and iterates on plans to combat violent extremism online, clear and open policies, firmly grounded in rule of law, that enhance transparency around content removal and account deactivations at home and abroad are critical to the protection of internet freedom.

In tackling hard problems like online extremism, governments must not create conditions that prevent companies from protecting and respecting users' rights. The Global Network Initiative (GNI), a multi-stakeholder organization focused on improving respect for freedom of expression and privacy by technology companies, recently published a set of recommendations for governments seeking to combat online extremism while also protecting internet freedom. In addition to adherence to international human rights law, such as the stipulation to satisfy necessity and proportionality requirements, GNI calls on governments to "ensure that counterterrorism laws and policies do not undermine the development and dissemination of messages by private actors that discuss, debate, or report on terrorist activities."[62] The policy brief also calls for government transparency about the "laws, legal interpretations and policies authorizing content restriction"[63] as well as about which agencies are legally permitted to authorize restrictions. Other recommendations include multi-stakeholder policy development and remedy mechanisms to "ensure that alleged violations" of individual expression made during efforts to restrict violent extremist speech "are investigated, and that effective remedies are available when such violations have occurred."[64]

> **Human rights groups and activists have documented numerous examples in which journalists, activists, and even innocent bystanders such as women named "Isis" have been victims of collateral censorship.**

In working with other governments and companies to develop effective policies for tackling online extremism, it is imperative that the U.S. government include civil society organizations in order to identify potential threats that measures may pose to the rights of internet users and to ensure protection of human rights online. Involvement of civil society organizations that focus on the protection of human rights (both online and offline) can ensure that governments do not unduly pressure companies to

In order to stop increasingly aggressive online censorship around the world, the U.S. government can reaffirm its commitment to limit liability for internet intermediaries and work to convince other governments to limit intermediary liability as a necessary part of their broader commitment to a free and open global internet.

remove content or accounts, and that appropriate remedy options are available.[65]

Beyond the problem of violent extremism, it is important that the United States promote general legal frameworks that maximize internet freedom. Limited liability for internet platforms is a key reason that the world's most trusted and powerful internet companies are headquartered in the United States.[66] The fact that U.S. law generally does not hold companies legally responsible for content published or transmitted by users is also broadly considered by legal scholars and freedom of expression advocates to be a key factor enabling social media platforms to create global spaces for freedom of expression, debate, and online assembly.[67] Yet many governments are now moving to increase liability for internet platforms.[68]

In order to stop increasingly aggressive online censorship around the world, the U.S. government can reaffirm its commitment to limit liability for internet intermediaries and work to convince other governments to limit intermediary liability as a necessary part of their broader commitment to a free and open global internet.

Finally, the Trump administration can advance internet freedom by **championing the importance of transparency and accountability around any restrictions of online speech.** This includes transparency and accountability about informal or private mechanisms that are used to restrict content on internet platforms in addition to actions taken via formal legal processes. If the government is going to encourage companies to use terms of service to restrict content that is otherwise legal, companies should also be expected to expand their transparency reports to disclose information about how terms of service are enforced, in addition to the volume and nature of content being removed. The government should be equally transparent about any informal or indirect requests being made to companies through private organizations that coordinate closely with government agencies.[69]

After leading by example, the next administration will then be in a strong position to urge other governments to maximize transparency about content restriction requests being made of companies. Governments committed to the advancement of internet freedom should also disclose the legal authorities or other mechanisms under which requests to restrict content are being made, in addition to releasing data on the volume and nature of requests. Research by the Ranking Digital Rights project has also identified instances in a number of democracies where the laws prevent companies from publishing transparency reports or other details about the number of government requests they receive to restrict content and other details about those requests, or where laws are so ambiguous that companies are not clear about what they can legally disclose.[70] We are not aware of any legitimate national security reason compatible with democratic and accountable governments that would justify restraint on the disclosure of such basic numeric information. The U.S. government should work with like-minded governments committed to internet freedom to promote

best practices in transparency around content restriction.[71]

✓ ***Ensure that U.S. sanctions and economic restrictions do not curtail connectivity***

The United States government has leveraged economic sanctions and export controls in order to respond to a wide range of challenges, from human rights abuses in Sudan to global cybercrime. In the most severe cases, these foreign policy instruments include nearly comprehensive restrictions on providing services or goods to individuals within certain countries. However, the United States has long recognized that humanitarian exemptions send a signal that such policies are designed to address certain regime behaviors, and not punish members of the public.

In response to the role of information technology in facilitating Iranians to contest allegations of electoral fraud and challenge state repression in 2009, the U.S. government created exemptions to the sanctions regime that allowed U.S. technology companies to offer services to users in Iran. These exemptions remain an enduring, bipartisan element of U.S. policy toward Iran, with protections for internet connectivity included even as Congress enacted more rigorous economic restrictions against Iran.[72] Throughout shifts in the relationship between Iran and the United States, protections for personal communications technologies have remained policy priorities that have evolved to enable U.S. technology companies to play a more effective role in promoting the free flow of information in Iran. In recognition of the principle that it is in the best interest of the U.S. to enable individuals in authoritarian countries to freely access information, these licenses have been extended to other sanctioned countries.

The personal communications exemptions and General Licenses enacted by the Treasury Department's Office of Foreign Assets Control (OFAC) have clearly contributed toward protecting and securing the free flow of information within sanctioned countries. Through providing a legal channel for American companies to engage such users, these policies ensure that users have alternatives to state-imposed platforms, such as Iran's national network, that more strongly respect their rights. Enabling American companies to provide internet connectivity and access to information services also provides competition to Chinese companies, promoting corporate social responsibility.

The Trump administration should continue this bipartisan legacy by continuing to build on the OFAC authorizations and exemptions that enable public-private partnership on internet freedom.

✓ ***Reform the Wassenaar Arrangement to ensure that export controls created to protect human rights do not negatively impact internet freedom***

The Wassenaar Arrangement, to which the U.S. is a signatory, is an international agreement which focuses on ensuring transparency and accountability in transfers of conventional arms and dual-use goods and technologies.[73] In 2013, the arrangement agreed to create two new export controls focusing on "cybersecurity items"[74] in an attempt to prevent the export of, among other things, dangerous hacking tools to specific states. Parties to the arrangement were eager to do something to stem the spread of dangerous intrusion technology that countries like Bahrain and Libya had purchased from foreign companies and used to target activists.[75]

However, although these changes may have been well-intended, the way the regulations were written poses a serious threat to cybersecurity. Legitimate security researchers, such as testers hired by a company to identify weaknesses in its systems, use the exact same tools. Under a broad implementation of the Wassenaar controls, these tools—and thus this work—could be criminalized.[76] internet freedom and security could be set back by years because of the way these controls would chill important security research, especially that done

by independent researchers who would be unable to comply with the complex regulations of an international agreement.

In early 2016, after receiving substantial criticism and deep opposition from the security research community and the technology industry more broadly, the House Oversight Committee held hearings on the issue and concluded that "there is a growing consensus that the export control language on cybersecurity intrusion and surveillance software and technology would have a devastating impact on cybersecurity efforts worldwide."[77] The Department of Commerce has withdrawn its proposed implementation, and the State Department has indicated its intention to renegotiate the language of the Wassenaar Arrangement.[78]

The Trump administration now has a window of opportunity to help guide a renegotiation of the Wassenaar Arrangement to ensure that export control rules strike a smarter balance that doesn't endanger critical security research.

2. People-Centric Security

Insecurity of person, data, and the inability to express oneself without censorship are all threats to internet freedom which the new administration must work to counter. Already, the United States has begun to work with other governments on the challenge of increasing security while protecting freedom. The U.S. government participates actively in the FOC's multi-stakeholder working groups, including Working Group 1, whose mission is to make policy recommendations to help governments and other stakeholders build and support "An Internet Free and Secure."[79] In October 2016 this working group, with representation from FOC member governments plus private sector and non-governmental stakeholders, published a set of principles for a "human rights based approach to cybersecurity." The document begins with a critique of the "dominant narrative" which falsely pits "privacy and other human rights against national security."[80]

According to FOC Working Group 1, "privacy and confidentiality of information are essential to the security of people, as well as to data, especially in the digital context where physical security and digital information are linked."[81] Indeed, security for networks and nations is not possible without strong protections for individual privacy and other human rights. The Trump administration should support the State Department's continued involvement with the FOC generally and participation in Working Group 1 specifically, along with the U.S. government's participation in other multilateral and multi-stakeholder internet policy development efforts. However, the new administration can demonstrate global leadership with a further step:

The Trump administration has an opportunity to integrate security, privacy, and human rights as indivisible pillars of a people-centric approach to national and global security in the internet age.

✓ *Support strong encryption for security and freedom*

Encryption is integral to the protection of internet freedom and for the security of individuals and organizations.[82] Increasingly, encryption is also a matter of public safety and plays an essential role in securing connected devices, such as transportation and medical equipment. Technically, encryption is the process of combining plaintext information, like files, emails, or text messages, with a secret mathematical key to scramble the content so that it becomes unintelligible to unauthorized users.[83] Encryption can be used to secure information in transit between users (end to end at its most secure)[84] or information stored on a physical device (data at rest).[85] The freedom to communicate or seek information in a secure manner is crucial for journalists, activists, and even regular citizens living in places where governments abuse surveillance powers against political opponents and economic rivals. Individuals who are unable to speak freely due to censorship or threats to their safety are empowered by the ability to express themselves anonymously through the use of encryption technology. When individuals know or believe that

they may be under surveillance, as is more likely when secure communications are unavailable, there is a demonstrable chilling effect on free speech and the free flow of information online.[86] Moreover, it is widely acknowledged that the growth of a secure internet has contributed positively to free expression[87] and that actions that prevent the use of secure, internet-based communications directly impede that same freedom.[88]

> **Increasingly, encryption is also a matter of public safety and plays an essential role in securing connected devices.**

A clear statement from the incoming administration that supports and promotes strong encryption would be an indicator of U.S. leadership in advancing internet freedom. Over the past eight years, the State Department has provided financial support to developers of encryption technologies as part of its mandate to support global internet freedom, but maintaining that support is insufficient to counter the mounting efforts by a growing number of governments—including some democracies—to undermine or even outlaw encryption. Countries like Bahrain,[89] Colombia,[90] Cuba,[91] and Pakistan[92] have restrictions on encryption, whether explicitly or implicitly, in laws governing national security or terrorism. Human rights violations committed by those governments are well documented. Yet, proposed legislation in countries like Australia, France, and the United Kingdom also threatens the ability of their citizens to secure their communications and data.[93]

When leaders of some of the world's oldest democracies refer to encryption as a national security threat and openly contemplate ways to circumvent it, all other governments—especially those with poor human rights records—are empowered to do the same. Meanwhile, insecure communication systems leave governments vulnerable to attack, and enable hackers to bring down services that people around the world depend upon.

The Trump administration should further affirm that it will not require companies to build "backdoors" for authorities to access encrypted products and services, thereby undermining their security and making them vulnerable to attack by criminals or state-sponsored actors. Concerns that the U.S. government has been working secretly to undermine encryption standards, and to imbed surveillance backdoors in consumer and enterprise technology, have eroded global trust in U.S. products. A 2010 document from the British intelligence and security agency GCHQ exposed by former National Security Agency (NSA) contractor Edward Snowden explained that "[f]or the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies" and "insert vulnerabilities into commercial encryption systems."[94] Other documents exposed by Edward Snowden revealed that the NSA was paying telecom companies like AT&T and Verizon for access to their networks,[95] and that companies like Apple, Google, and Microsoft were participating in the PRISM surveillance program.[96] More recently, U.S. government officials have criticized Google and Apple for encrypting their mobile operating systems[97] and requested that Apple undermine the security of its iOS software to cooperate with the FBI.[98]

Trust in U.S. technology companies, and trust in the intentions of U.S. intelligence and law enforcement agencies, has plummeted—not only domestically, but around the world.[99] International consumers are concerned that potential vulnerabilities in technology developed in the United States would not only put them at risk of exposure to U.S. surveillance, but those same backdoors could be used other actors and threaten their security and safety. A backdoor for the NSA could be opened by state-sponsored hackers working for China, Ethiopia, Iran, or other governments that regularly surveil and repress their own citizens.

A strong stand against backdoors by the new administration would not only help to strengthen internet freedom; it would be an important step toward rebuilding global public trust in U.S. companies that produce the vast majority of consumer technology products and in the strong encryption that they seek to offer their customers around the world.

✓ *Work to make surveillance power accountable*

International trust in the United States as a leader in the internet freedom space has greatly diminished since Edward Snowden released evidence of mass surveillance by intelligence agencies in the U.S. and United Kingdom.[100] Documents revealed that the NSA (and partner agencies from allied countries known as the "Five Eyes") were conducting surveillance on hundreds of millions of people every day.[101] Further, much of this activity was taking place outside of the legal frameworks designed to protect privacy and civil liberties.

Pervasive digital surveillance threatens the privacy of citizens both within and outside of the United States, and this sweeping disregard for electronic privacy has particularly troubling implications for internet freedom.[102] In the digital age, freedom of expression cannot be fully exercised if the individual's right to privacy is violated by overbroad, pervasive surveillance.[103]

Freedom House's 2015 *Freedom on the Net* report noted that over the preceding one-year period, governments in 14 of 65 countries included in the report—roughly 20 percent— passed new laws to increase surveillance capabilities.[104] Around the world, information is collected on individuals, many of whom are targeted for their religious beliefs or for their opposition and criticism of government activities, often without clear oversight or transparency. In repressive regimes, journalists, activists, and others face repercussions for emails, Tweets, blog posts, and other non-anonymous internet behavior tracked by their governments. Vulnerabilities in mobile phone software, for example, have been exploited to spy on a human rights defender working in the United Arab Emirates.[105] Journalists have had their Telegram accounts hijacked to infect their contacts with malware.[106] Many individuals who face these serious threats for themselves and their sources are forced to rely on complex, and sometimes still fallible, security technologies to stay out of jail—or alive.[107] No amount of State Department funding and training for secure tools that help keep activists and journalists in repressive regimes safe can make up for the broader technological and legal trends that are making surveillance more globally pervasive by the day—unless and until the U.S. government takes bold steps at home and abroad to improve accountability and transparency around government surveillance.

Pervasive digital surveillance threatens the privacy of citizens both within and outside of the United States, and this sweeping disregard for electronic privacy has particularly troubling implications for internet freedom.

The United States must first lead by example: Reform domestic surveillance laws to limit their scope and improve transparency. Two specific surveillance authorities, Section 702 of the Foreign Intelligence Surveillance Amendments Act[108] and Executive Order 12333[109], are especially egregious and should be targeted for reform. Section 702 is technically supposed to be used for targeting non-U.S. persons outside of the United States, when the data is in the U.S., but documents leaked by Edward Snowden revealed that 702 was being used far more expansively than expected. It has served as the legal basis for the collection of huge amounts of telephone and internet traffic passing through, or stored within, the United States,[110] and even though it is supposedly for use against foreign targets, Section 702 surveillance also incidentally

The United States must first lead by example: Reform domestic surveillance laws to limit their scope and improve transparency.

collects the communications of Americans—without a warrant.[111]

Executive Order 12333 authorizes collection of the content of non-U.S. persons' communications, not just metadata, that takes place outside of the United States.[112] Millions of innocent foreigners' communications are collected abroad, and because internet communications increasingly travel across U.S. borders, and are commonly stored elsewhere, this information will also inevitably contain the communications of U.S. citizens.[113] Reforms made to more narrowly target subjects of an investigation, instead of collecting such broad swaths of data, could help minimize harms created by pervasive government surveillance programs, both in the United States and internationally. Also, ensuring that the use of the information collected is limited to national security and counterintelligence investigations would mitigate incidental collection.

Enhancing transparency around these practices, and reporting to the public retrospectively on requests made to companies for user information and other actions to assist in surveillance, such as storing user data or modifying technology, will help demystify these practices. It will also enable the government to take responsibility for the impact that surveillance has had on the privacy of Americans, as well as non-U.S. persons, in the name of national security. Clarifying facts around questions like how many Americans' information is collected, how many non-U.S. persons information is collected, how long information is retained, and how many requests for user information are made to internet and telecommunications companies, provide transparency, accountability, and allow for a productive conversation about the costs of electronic surveillance and the extent to which citizens can accept those costs in the name of security.

The public debate sparked by the Snowden revelations about surveillance, national security, and civil liberties is not unique. Democracies across the world are struggling with the question of how to address legitimate law enforcement and national security needs while ensuring that surveillance laws and practices are accountable to the public interest and compatible with fundamental human rights principles. This is one of the most difficult global governance questions of our time. It is vital for the future of internet freedom and democracy itself that nations committed to the idea of a free and open internet work together to ensure that surveillance laws and practices enable law enforcement and security agencies to do their jobs without weakening democracy and human rights.

As we undertake the difficult work of surveillance reform at home, **the United States must also lead a global conversation about the appropriate relationship between surveillance, democracy, and accountable governance.** In order to reverse the current erosion of internet freedom, governments must work together, with their own citizens, security experts, global human rights advocates, and the private sector, to ensure that governments' surveillance powers do not undermine citizens' ability to hold them accountable or undercut the public trust necessary to maintain the economic and social value of internet-connected technologies.

In April 2014 in Tallinn, Estonia, nearly a year after the first Snowden revelations were first published, the U.S. and other FOC member governments issued the Tallinn Recommendations for Freedom Online. Responding to political critics at home, and global stakeholder concerns that they had failed to live up to their own commitments to internet freedom, member governments reaffirmed their allegiance to the idea of an open and interoperable internet.

They also called upon "governments worldwide to promote transparent and independent, effective domestic oversight related to electronic surveillance…while committing ourselves to do the same."[114] The new administration should clearly and publicly affirm its intention to start working immediately with other democratic governments to implement this commitment. If leading democracies can demonstrate concrete progress—no matter how incremental—they will benefit from the goodwill and support of citizens and global stakeholders who recognize that this is a hard problem, but whose own prosperity and freedom ultimately depend on democracies' success in holding surveillance power accountable.

What would concrete progress look like? In 2015 a multi-stakeholder working group of experts from Germany and the United States, supported by the German Marshall Fund, suggested a number of concrete steps for governments committed to holding surveillance power accountable can take.[115] They include:

- Publish official interpretations of the legal authorities under which surveillance is authorized,
- Increase staffing and budget of institutions that authorize and oversee surveillance,
- Set and implement public standards for publishing all non-classified elements of surveillance authorizing decisions and related oversight reports,
- Require regular public reporting by all public agencies about the number, type, and purpose of interception requests, number of people or communications affected, and the criteria used to authorize the surveillance.[116]

The FOC's Working Group 3, focused on "Privacy and Transparency Online," has developed a "people-centric standard" for transparency by companies and governments on a range of actions they take affecting online freedom, including how internet users' personal information is accessed, handled and shared.[117] While many companies now engage in what has come to be known as "transparency reporting" on requests that governments make to hand over user information or restrict content (see the previous section for more on the latter) few governments have made an effort to report in parallel about requests they are making to companies.[118] The Trump administration should work with fellow FOC members to make government transparency about surveillance laws and practices, along with strong oversight mechanisms, a standard and expected feature of open and democratic societies.

✓ *Improve frameworks for cross-border law enforcement requests*

Because the internet and the commercial platforms that use it span across national borders, it is increasingly common that law enforcement authorities investigating crimes in one jurisdiction need access to user information stored in other jurisdictions. Cross-border agreements called Mutual Legal Assistance Treaties (MLATs) have long been the traditional way for law enforcement officials outside of the U.S. to request evidence stored inside the U.S. However, these treaty mechanisms are currently failing to keep up with the massive internet-driven increase in demand, which raises the possibility that foreign governments could react by taking unilateral actions that may negatively impact both human rights and American businesses internationally. Some sort of reform is clearly needed. However, **any reform of the MLAT process to better foster law enforcement access to data across borders must not be allowed to substantially diminish the privacy protections currently afforded to international users of U.S. services.**

MLATs are formal agreements between countries that create international legal obligations to help one another in conducting criminal investigations and prosecutions. When law enforcement officers or prosecutors need help to obtain evidence held in another country, a designated government agency

makes a formal request, and the corresponding organizations in the other country work together to retrieve the requested evidence.[119]

Non-U.S. governments wishing to gain access to data held by U.S. companies have to meet U.S. criminal justice standards, including the probable cause requirement of the U.S. Constitution's Fourth Amendment.[120] The MLAT system also involves the approval of an independent magistrate in the U.S. before a data demand is issued. In addition, while MLAT treaties do not carry "dual criminality" requirements as extradition treaties often do, they are subject to a less specific "political offense" exception that can be used to deny requests on human rights grounds or where the information would be targeted at dissidents or minority communities.[121] These protections of U.S. law thereby extend to citizens around the world when they use U.S.-based online cloud providers. In these ways, MLATs protect the privacy and human rights of people around the world who use U.S.-based online services—and in doing so also provide a competitive benefit to those U.S. companies compared to those operating in countries with less protective legal standards.

In the past, the use of MLATs was relatively rare because the number of criminal cases that turned on evidence located in another country was relatively few. However, the rise of the internet, combined with the historical forces that combined to place many of the world's internet companies in the United States, have led to an explosion of MLAT requests. In its fiscal year 2015 budget request, the DOJ stated that the preceding decade had seen an increase in MLAT requests of almost 60 percent, and computer requests in particular had exploded by tens.[122] Compounding these issues are complex questions of jurisdiction that arise from the fact that many U.S. companies store their data in a variety of data centers located around the world, but consider themselves under only U.S. jurisdiction.[123]

This dramatic increase in the number of MLAT requests to the U.S. has slowed the system to the point where a single request can take up to 10 months to complete.[124] These increasing delays in the face of increased need, added to the growing political pressure from sovereign nations frustrated by having to consult with the U.S. government and meet its legal standards in order to investigate so many purely domestic crimes, have caused serious tension—especially between foreign law enforcement and U.S. companies that are legally unable to disclose their customers' communications without U.S. legal process. This frustration is leading many foreign governments to contemplate or enact policies that would threaten cybersecurity, human rights, the free flow of information—policies such as mandatory data localization, encryption backdoor mandates, localized routing requirements, or the aggressive enforcement of extraterritorial demands on U.S. companies leading to the jailing of U.S. executives.[125]

This dramatic increase in the number of MLAT requests to the U.S. has slowed the system to the point where a single request can take up to 10 months to complete.

A potential new model for handling cross-border data requests was recently proposed as a joint U.S-U.K. bilateral agreement. That draft agreement from the DOJ, which would require implementing legislation, would allow U.S. companies to voluntarily respond directly to U.K. legal demands (and U.K. companies to respond to U.S. demands), including not only demands for stored data but even for real-time wiretapping.[126] Some expert commentators have cautiously suggested that this voluntary model allowing foreign countries to bypass the MLAT process altogether may be a reasonable solution.[127] However, the deal as proposed would also substantially weaken or eliminate most of the privacy and human rights protections that MLATs currently provide to customers of U.S. companies, while also creating new threats to the privacy of Americans too.[128]

The administration should work with Congress to pass the widely-supported bipartisan Email Privacy Act which would clarify that U.S. law enforcement needs to get a warrant in order to seize emails and other electronic communications stored by U.S. companies, and would close other key gaps in current U.S. privacy law.

Combined with the fact that the U.S. has much less of a need for cross-border data than the U.K. does, and the fact that this agreement wouldn't specifically preclude the U.K. from *also* adopting additional measures that would threaten U.S. companies and the free flow of information—up to and including jailing U.S. executives if its demands are not complied with—it is clear that this proposed agreement in its current form would be a bad deal for America. So too is the legislation proposed by the DOJ that would allow for the same type of dangerous agreement with many other countries.[129]

Reforming the system of cross-border law enforcement requests in a manner that addresses the needs of law enforcement while also preserving internet freedom will not be easy, but we have to get it right. It is important to ensure that any new treaties, and requests under them, comply with international human rights standards, and that those requests provide substantive and procedural protections that are comparable to the U.S. search warrant standards that have long protected data stored in the U.S. A first step in the right direction would be to reform the U.S.'s own laws governing law enforcement access to digital evidence, to provide a stable basis on which to build a new cross-border regime that respects Americans' civil liberties and the human rights of U.S. customers around the world. The administration should therefore work with Congress to pass the widely-supported bipartisan Email Privacy Act which would clarify that U.S. law enforcement needs to get a warrant in order to seize emails and other electronic communications stored by U.S. companies, and would close other key gaps in current U.S. privacy law.[130]

3. Accountable Multi-Stakeholder Governance

On October 1, 2016 the contract between the U.S. Department of Commerce and ICANN to carry out the Internet Assigned Numbers Authority (IANA) functions expired. Oversight of the coordination of critical technical functions that enable people around the world to send e-mails and access websites across distributed inter-connected networks without centralized control has now passed from nominal U.S. stewardship to that of an international, multi-stakeholder community.

Despite eleventh-hour opposition by a few vocal members of Congress who felt that the transition away from U.S. oversight of the IANA functions would jeopardize internet freedom, there was strong bipartisan support for a multi-stakeholder vision of global internet governance developed and promoted by successive Republican and Democratic administrations over nearly two decades.[131] The transition was supported by a wide range of companies and members of the technical community as well as a number of civil society and human rights groups whose core areas of work include promotion of and support for internet freedom. [132] This support reflected broad agreement that the transition as designed by the Department

of Commerce was in fact the best way to minimize the threat to internet freedom from the authoritarian visions of countries such as Russia and China.[133]

While the IANA transition was necessary—both as fulfillment of a U.S. commitment to the international community and to prevent greater problems in the long run—it is not without risk. In order to ensure the success of multi-stakeholder internet governance for a free and open global internet, the next administration should:

✓ ***Strengthen ICANN's independence, accountability, and transparency***

Strengthen mechanisms that ensure the independence, accountability and transparency of ICANN's decision-making processes.

ICANN has been the target of valid criticism for insufficient transparency and accountability since its inception.[134] One of the U.S. conditions for the IANA transition was implementation of stronger accountability mechanisms and processes.[135] The new ICANN bylaws contain commitments to greater board transparency, staff accountability, diversity, among others. In order to implement these commitments, two work streams were established, to be carried out by government representatives and other stakeholders: The first was mostly completed when the transition took place while the second is ongoing.

The new ICANN bylaws also contain a commitment to human rights, although the "framework of implementation" remains under development by a multi-stakeholder working group formed in June 2016.[136] Whether that framework, and the implementation frameworks for ICANN's other commitments, are sufficiently robust and compatible in fostering a free and open global internet depends in large part on the individuals participating in these working groups, as well as the relationships between the working groups and ICANN's other policy development and decision making processes. The U.S. government has been a participant in both work streams, enabling a continued U.S. role in strengthening ICANN's accountability mechanisms as they are designed and implemented in the future.[137]

The new ICANN bylaws have also vested new powers in the ICANN community, including the power to reject budgets and strategic plans, remove or replace board members or even the entire ICANN board, or even seek an alternative to ICANN to perform the IANA functions. The purpose of these new powers is to give the multi-stakeholder community the ability to hold ICANN accountable much as the U.S. government did through its former oversight role prior to the transition. The efficacy of these oversight powers will be tested over the next few years. Also to be tested are the mechanisms aimed at preventing any one set of interests or stakeholders from seizing control over or hijacking these powers.[138] The U.S. has a role to play in assuring that the oversight system meets its intended objectives.

✓ ***Work to ensure diversity and independence of ICANN stakeholders***

The next administration can advance internet freedom by working with the private sector and other governments to build independent and accountable financial support mechanisms that will ensure diversity of stakeholder participation in ICANN.

In order to garner broad international trust, ICANN must have robust participation from all regions of the world, with sufficient resources provided to support participation from small businesses, non-governmental organizations, and academia. Like most governance institutions, ICANN's multi-stakeholder governance model is vulnerable to capture by whichever entities that can devote the greatest resources to participating in all levels of deliberation and decision-making. In other words, while anybody from anywhere with any institutional affiliation (or none) can show up and participate in ICANN meetings, those who are able to dedicate the greatest number of resources and person-hours to committees, conference calls, and

travel to attend several in-person meetings every year have a higher chance of seeing their interests and positions prevail. Multinational corporations and well-resourced governments motivated by strong political or geopolitical agendas (including authoritarian actors who do not share the United States' vision of a free and open global internet) have an advantage in multi-stakeholder settings unless resources and political will are committed to counter inevitable imbalances of resources, personnel, and political power. Support for diverse participation should extend to other multi-stakeholder internet governance and standards-setting institutions and processes.

✓ ***Strengthen the multi-stakeholder Internet Governance Forum***

At the 2005 UN World Summit for the Information Society (WSIS), the United States played a key role in the negotiation of an eleventh-hour agreement to maintain ICANN's stewardship of the global internet addressing system, thereby halting concerted efforts by a group of nations including China to shift ICANN's functions to from the multi-stakeholder organization to a UN body, the International Telecommunications Union (ITU). That agreement also created the UN Internet Governance Forum (IGF), an annual conference where stakeholders from around the world come together to discuss a wide range of internet issues including its governance, "use and misuse," but with no decision-making power or mandate.[139]

It is in the U.S. government's long term interest to support the IGF's continuation and to strengthen its effectiveness.

From its first meeting 10 years ago, the IGF has become a unique forum where business, government, civil society activists, and members of academia and the technical community from all over the world meet on an equal footing to discuss and debate solutions to pressing internet policy issues of the day. Regional and national IGFs have proliferated around the world, contributing to bottom-up policy dialogues that bring small business entrepreneurs and grassroots activist groups into the same room with key actors in government ministries and multinationals. The IGF has been described not only as an "observatory" but also a "clearing house" for new policy ideas emerging from the grassroots, and even an "early warning system" for problems that can turn into crises if not addressed.[140]

However the IGF faces challenges. Even though it has no decision-making authority—which is key to its role as an incubator of sorts for internet policy ideas—the IGF's future depends on whether the annual conferences can demonstrate long-term value for participants as well as tangible (if indirect) policy impact. Improved accountability and transparency of its operations are important for maintaining trust among a diverse group of global stakeholders upon whose participation its success depends. The forum also needs to demonstrate a clearer link between the ideas it helps to incubate and the implementation of internet policy innovations around the world.[141]

Having played a role in the IGF's creation, the United States also has an important role to play in the IGF's long-term success. Its success will not only help the U.S. build coalitions among public and private stakeholders in support of specific initiatives and policies to advance internet freedom. U.S. leadership in supporting the IGF is also vital in helping to inoculate the emergent multi-stakeholder internet governance system from attack by major world powers that continue to argue that important decisions about the internet's future should be made primarily by governments.

Strengthening the IGF's effectiveness and capacity for policy innovation and impact is thus an important pillar of the long-running U.S. efforts over the course of successive Republican and Democratic administrations to prevent authoritarian countries from gaining international support in their efforts to shift control of key internet governance functions away from multi-stakeholder bodies such as ICANN into the hands of UN bodies such as the ITU.

✓ ***Build stronger accountability mechanisms into the Freedom Online Coalition.***

At a time when U.S. motivations for supporting multi-stakeholder governance and internet freedom are being questioned by geopolitical challengers,[142] it is important to demonstrate through concrete action that U.S. commitment to the multi-stakeholder model is in the interest of people around the world (not just Americans). This will in turn help to strengthen support amongst stakeholders around the world for a new approach to global governance in which non-state actors are granted more voice and power to shape the internet's future.

The FOC is an ideal place to start, given its origins and mandate.[143] **If the United States is to be a credible leader in advancing global internet freedom it must work to ensure that institutions such as the FOC demonstrate tangible progress in advancing global internet freedom.**

An independent assessment of the coalition's work points to two main achievements: improved coordination between member countries' foreign ministries on internet freedom related policy matters and the creation of a dedicated fund to assist civil society activists and journalists struggling against censorship and surveillance under repressive regimes.[144] Yet at the same time, since joining the coalition several member countries have enacted policies and laws that contribute to the erosion of global internet freedom.[145] There is no mechanism to evaluate whether member countries have lived up to joint commitments that include a call for "governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content takedown notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same."[146] Nor is there a mechanism to hold governments accountable to these commitments. Multi-stakeholder working groups produce policy recommendations in furtherance of members' stated commitments, but members have no obligation to consider, let alone act upon, them and there is little evidence that they have done so.[147]

One way to incentivize and demonstrate the FOC's tangible impact on internet freedom is by building multi-stakeholder accountability mechanisms into—or alongside of—the FOC. One way to do this would be to adopt some elements of the Open Government Partnership (OGP), a multilateral initiative that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance, whose membership overlaps heavily with the FOC. For example, members of the OGP commit to develop National Action Plans, articulating what concrete steps they will take over a two year period to meet their commitments followed by a multi-stakeholder evaluation process to assess how well the plan was enacted. FOC members could develop similar plans for how they will make a positive contribution to global internet freedom.[148]

The FOC could also concretely advance internet freedom by supporting the creation of an affiliated multi-stakeholder transparency reporting initiative modeled after the Extractives Industry Transparency Initiative (EITI), launched in 2002 by the U.K. government, through which governments report payments they receive from oil, gas, mining, and other extractive industry companies, and companies report on payments they make to governments.[149] An internet freedom-advancing equivalent of the EITI would coordinate and assess parallel transparency reports by governments and companies: with governments publishing data about the number of requests made to companies for user data or to restrict content, and companies publishing data about the number of requests received and how those requests were handled. Members of the FOC's Working Group 3 on Privacy and Transparency Online have been developing frameworks and recommendations for how governments and companies can improve transparency reporting which and could be used as the basis to build a systematic framework for transparency and accountability.[150]

CONCLUSION

The recommendations in this paper have focused on areas where the United States not only can—but *must*—assert stronger global leadership. Without such leadership, the state of global internet freedom is likely to continue on its present trajectory of decline and deterioration. The incoming administration now leads a country that has, for over 25 years, been at the forefront of technological innovation and has benefited from its effects on trade and commerce, technological innovation, health, safety, education, and diplomacy. Working to advance internet freedom will help preserve those gains, and secure the United States' role as the shaper of the future global internet policy.

Support for the promotion of internet freedom cuts across partisan lines and provides an opportunity for cooperation with Democrats, Republicans, Libertarians and Independents in the private and nonprofit sectors. The framework that this paper recommends will enable the U.S. government to craft policies that address the biggest challenges to the internet's future. Although the list of issues is not exhaustive, this paper articulates why, how, and on what issues the United States can and should assert leadership. The U.S. can lead the world through example, working cooperatively to ensure the free flow of information at home and across the world: We can expand access to the infrastructure needed to connect to the internet, and insure that people around the world have access to an internet that is not restricted or blocked by oppressive governments. The Trump administration can assert global leadership by integrating security, privacy, and human rights as indivisible pillars of a people-centric approach to national and global security in the internet age, protecting individuals from expanded surveillance and giving them the opportunity to use tools like encryption. The administration is well positioned to work with other governments, private sector businesses, and non-governmental organizations to govern the internet in a transparent and accountable way.

In today's digitally interconnected world, a strong leadership position on internet freedom is not only important—it is a necessary component of America's global economic and geopolitical leadership.

A commitment from the Trump administration to promote and protect internet freedom, at home and abroad, will be consistent with this nation's long standing international commitments to uphold human rights and the rule of law while also strengthening our economy and protecting us from threats to national security.

Leadership on internet freedom will send a powerful signal to the rest of the world that the United States is committed to supporting technological innovation, and will be a leader in promoting policies that maintain the internet as a vital community lifeline and modern, global marketplace.

Notes

1 Philip N. Howard and Muzammil M. Hussain, *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. Oxford Studies in Digital Politics, [Oxford, N.Y: Oxford University Press, 2003].

2 Pamela B. Rutledge, "Why Social Media Matters in the Paris Terrorist Attacks," *Psychology Today*, November 15, 2015. https://www.psychologytoday.com/blog/positively-media/201511/why-social-media-matters-in-the-paris-terrorist-attacks; Danielle Paquette, "How Facebook Tried to Help Paris Users Reach Their Loved Ones," *Washington Post*, November 14, 2015. https://www.washingtonpost.com/news/wonk/wp/2015/11/14/how-facebook-tried-to-help-paris-users-reach-their-loved-ones/?tid=a_inl&utm_term=.93ad0f6d68f7

3 Dina Fine Maron, "How Social Media Is Changing Disaster Response," *Scientific American*, June 7, 2013. https://www.scientificamerican.com/article/how-social-media-is-changing-disaster-response

4 Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, [Cambridge, Mass: MIT Press, 2008]; Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, [Cambridge, Mass: MIT Press, 2012]; Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Cambridge, MA: MIT Press; McChesney, Robert Waterman. 2013. *Digital Disconnect: How Capitalism Is Turning the Internet against Democracy*. (N.Y.: The New Press); Carr, Madeline. 2013. "Internet Freedom, Human Rights and Power." *Australian Journal of International Affairs* 67 (5): 621–37.

5 Giampiero Giacomello, *National Governments and Control of the Internet: A Digital Challenge*. Routledge Research in Information Technology and Society, [New York, NY: Routledge, Taylor & Francis Group, 2005], Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, [Boston, Mass.: The MIT Press, 2010]; Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91 (1): 111–30.

6 See *Freedom on the Net 2016: Silencing the Messenger: Communication Apps Under Pressure*," Freedom House, 2016. https://freedomhouse.org/report/freedom-net/freedom-net-2016 (discussing the impact of limited availability of encryption and anonymity services on activists, journalists, minorities, and others)

7 Aaron Pressman, "Why Telecom Carriers Are Resisting a Program for Low-Income Internet Subsidies," *Fortune*, December 1, 2016. http://fortune.com/2016/12/01/fcc-att-verizon-lifeline-broadband

8 Global Online Freedom Act of 2013, HR 491, 113th Cong., 1st sess,. https://www.congress.gov/bill/113th-congress/house-bill/491

9 Shawn M. Powers, and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom. History of Communication*, [Urbana, Ill: University of Illinois Press, 2015].

10 An initiative launched by then-Secretary of State Hillary Clinton in 2011. See https://www.freedomonlinecoalition.com/.

11 Christopher Painter, Daniel Sepulveda, and Uzra Zeya, "Internet Freedom For All," *DipNote*, August 13, 2013. https://blogs.state.gov/stories/2013/08/13/internet-freedom-all

12 "Statement of Rep. Chris Smith, Introducing the Global Internet Freedom Caucus," March 9, 2010. http://chrissmith.house.gov/uploadedfiles/2010-03-09_statement_on_global_internet_freedom_caucus.pdf; "Senators Announce Formation of Global Internet Freedom Caucus," March 24, 2010. https://www.casey.senate.gov/newsroom/releases/senators-announce-formation-of-global-internet-freedom-caucus

13 Laura DeNardis, "The Emerging Field of Internet Governance," Yale Information Society Project Working Paper Series, September 17, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343

14 ITU. 2005. "WSIS Outcome Documents." December, para. 35, p. 75. https://www.ourinternet.org/report#4

15 "U.N. Human Rights Council: First Resolution on Internet Free Speech," July 5, 2012. http://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech

16 UN Universal Declaration of Human Rights, available at http://www.un.org/en/universal-declaration-human-rights.

17 UN International Covenant on Civil and Political Rights. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

18 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank LaRue," UN General Assembly Human Rights Council, A/HRC/23/40, April 17, 2013. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf; Rebecca MacKinnon, Elonnai Hickok, Allon Bar, and Hae-in Lim, "Fostering Freedom Online: The Role of Internet Intermediaries," UNESCO, 2014. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

19 "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," UN Human Rights: Office of the High Commissioner, June 16, 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

20 Freedom Online Coalition. https://www.freedomonlinecoalition.com

21 Freedom on the Net 2016, 1.

22 Deibert, "The Geopolitics of Cyberspace After Snowden," *Current History* [January 2015]: 9-12.

23 "#KeepItOn," Access Now. https://www.accessnow.org/

keepiton

24 Deibert, "The Geopolitics of Cyberspace After Snowden."

25 "About Filtering," OpenNet Initiative. https://opennet.net/about-filtering

26 Miklos Haraszti, "Forward," *Access Controlled*, eds. Deibert, Palfrey, Rohozinski, Zittrain [Cambridge, Mass: MIT Press, 2012].

27 Jon Brodkin, "ISP lobby has already won limits on public broadband in 20 states," *Ars Technica*, February 12, 2014. http://arstechnica.com/tech-policy/2014/02/isp-lobby-has-already-won-limits-on-public-broadband-in-20-states

28 "The Broadband Technology Opportunities Program: Expanding Broadband Access and Adoption in Communities Across America, Overview of Grant Awards," National Telecommunications and Information Administration, 2010, 2. https://www.acuta.org/acuta/legreg/122110a.pdf

29 NTIA, "The Broadband Technology Opportunities Program," 3-4.

30 Michael Calore, "Mosaic Browser Lights Up Web With Color, Creativity," *Wired*, April 22, 2010. https://www.wired.com/2010/04/0422mosaic-web-browser

31 George Bush, "Remarks on Signing the High-Performance Computing Act of 1991," December 9, 1991. http://www.presidency.ucsb.edu/ws/?pid=20320

32 George Bush, Remarks on Signing the High-Performance Computing Act of 1991.

33 Brian Fung, "Dig once: The no-brainer Internet policy the White House just endorsed," *Washington Post*, September 22, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/09/22/dig-once-the-no-brainer-internet-policy-the-white-house-just-endorsed

34 "Minimizing Excavation Through Coordination," FHWA Office of Transportation Policy Studies, October 2013. https://www.fhwa.dot.gov/policy/otps/policy_brief_dig_once.pdf

35 Austin Coleman, "Dig Once: Using Public Rights-of-Way to Bridge the Digital Divide," The Current State E-Newsletter, November/December 2016. http://www.csg.org/pubs/capitolideas/enews/cs41_1.aspx; GAO- 12-687R; Broadband Conduit Deployment, Government Accountability Office, June 27, 2012. http://www.gao.gov/assets/600/591928.pdf

36 Council of State Governments. http://www.csg.org/pubs/capitolideas/enews/cs41_1.aspx

37 "U.S. State Department Launches Global Connect Initiatives at UNGA," U.S. Department of State, September 27, 2015. http://www.state.gov/r/pa/prs/ps/2015/09/247374.htm

38 "Global Connect Initiative: Building Global Support (list of participating civil society organizations)" https://share.america.gov/wp-content/uploads/2016/04/5.-GCI-Building-Global-Support-FINAL.pdf

39 "Global Connect Initiative: Global Connect Principles." https://share.america.gov/wp-content/uploads/2016/04/1.-GCI-Connectivity-Principles-FINAL.pdf

40 "Global Connect Initiative: Global Connect Roadmap." https://share.america.gov/wp-content/uploads/2016/04/2.-GCI-Road-Map-FINAL.pdf

41 "Global Connect Initiative: Global Connect Roadmap."

42 David Kaye and Brett Solomon, "Merely Connecting the Developing World to the Internet Isn't Enough," *Slate*, October 13, 2015. http://www.slate.com/blogs/future_tense/2015/10/13/the_u_n_wants_to_connect_the_world_to_the_internet_that_s_not_enough.html

43 "The Human Rights Principles for Connectivity and Development," Access Now, December, 2016. https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf

44 See "Civil Society Statement on the Launch of the Global Connect Initiative," Best Bits, September 24, 2015. http://bestbits.net/global-connect-initiative; "Letter to Ministers of Finance on Global Connect initiative," Best Bits, April 2016. http://bestbits.net/finance-ministers-global-connect

45 Digital GAP Act, HR 5537, 114th Cong., 2nd sess., September 8, 2016. https://www.congress.gov/bill/114th-congress/house-bill/5537/text

46 Cathy McMorris Rodgers and Ed Royce, "A 'Build-Once' Policy for the Developing World," Recode, September 13, 2016. http://www.recode.net/2016/9/13/12889726/digital-gap-act-build-once-policy-developing-world-ebola-zika.

47 Nart Villeneuve, "The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace," *First Monday*, 2006. http://firstmonday.org/ojs/index.php/fm/article/view/1307/1227 Also see: Deibert, et al. eds., *Access Denied.*

48 Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* 14, February 2009, http://firstmonday.org/article/view/2378/2089; Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled*, eds. Deibert, et al. [Cambridge, Mass: MIT Press, 2012], 71-85; Rebecca MacKinnon, "China's Networked Authoritarianism," *Journal of Democracy* 22, [April 2011]: 32-46. https://muse.jhu.edu/article/427159/pdf.

49 "Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy," Freedom House, 8. https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf

50 "Twitter Sees Surge in Government Requests for Data," BBC, February 10, 2015. http://www.bbc.com/news/technology-31358194; Devin Coldewey, "Google's Latest Transparency Report Sets More Records in Government Request Numbers," Tech Crunch, October 12, 2016. https://techcrunch.com/2016/10/12/googles-latest-transparency-report-sets-more-records-in-government-request-numbers; Katie Collins, "Facebook sees spike in government requests for data, content restriction," CNet, November 12, 2015. https://www.cnet.com/news/facebook-sees-spike-in-government-requests-for-data-

and-content-restriction

51 Rebecca MacKinnon, Elonnai Hickok, Allon Bar, and Hae-in Lim, "Fostering Freedom Online: The Role of Internet Intermediaries," UNESCO, 2014. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

52 "Freedom of Expression: Limitations," Article 19. https://www.article19.org/pages/en/limitations.html

53 MacKinnon et al., "Fostering Freedom Online."

54 Christ Ducket, "India triples content banning on Facebook as governments increase user data requests," ZD Net, November 12, 2015. http://www.zdnet.com/article/india-triples-content-banning-on-facebook-as-governments-increase-user-data-requests; Felicity Capon, "Germany Ranks Third Highest for Censorship on Twitter," *Newsweek*, February 11, 2015. http://www.newsweek.com/germany-ranks-third-highest-tweet-censorship-306148; "Freedom on the Net 2016: India, Brazil, France and Germany."

55 "Freedom on the Net 2016: Russia and Thailand."

56 "European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech," European Commission, May 31, 2016. http://europa.eu/rapid/press-release_IP-16-1937_en.htm; Alex Hern, "Facebook, YouTube, Twitter and Microsoft Sign EU Hate Speech Code," *Guardian*, May 31, 2016. https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code

57 "Frequently Asked Questions: Stronger Action at EU Level to Better Tackle Violent Radicalisation," European Commission, June 14, 2016. http://europa.eu/rapid/press-release_MEMO-16-2179_en.htm

58 "Factbox: How U.K,'s Anti-terrorism Internet Unit Works," Reuters, October 4, 2010. http://www.reuters.com/article/us-security-internet-factbox-idUSTRE6932AY20101004

59 Rebecca MacKinnon, "In Age of ISIS, Will You Lose Web Freedoms of Arab Spring?" CNN, January 24, 2016. http://www.cnn.com/2016/01/24/opinions/social-media-five-years-anniversary-arab-spring-mackinnon; Courtney C. Radsch, "Privatizing censorship in fight against extremism is risk to press freedom," Committee to Protect Journalists, October 16, 2015. https://cpj.org/blog/2015/10/privatizing-censorship-in-fight-against-extremism-.php; "Input from the Committee to Protect Journalists to the Office of the High Commissioner for Human Rights Concerning Resolution 30/15 of the Human Rights Council on Human Rights and Preventing and Countering Violent Extremism," Committee to Protect Journalists, March 18, 2016. https://cpj.org/campaigns/2016.03.18_CPJ_CVE_submission_OHCHR.pdf

60 "UN Expert Warns Combat Against Violent Extremism Could Be Used as 'Excuse' to Curb Free Speech," UN News Centre, May 3, 2016. http://www.un.org/apps/news/story.asp?NewsID=53841; "Letter to European Commission on Code of Conduct for "Illegal" Hate Speech Online," Center for Democracy & Technology, August 17, 2016. https://cdt.org/insight/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online

61 "As White House and Tech Companies Meet on Terrorism, Privacy & Human Rights Organizations Demand Seat at Table," New America's Open Technology Institute, March 8, 2016. https://www.newamerica.org/oti/press-releases/as-white-house-and-tech-companies-meet-on-terrorism-privacy-human-rights-organizations-demand-seat-at-table

62 "Extremist Content and the ICT Sector A Global Network Initiative Policy Brief," Global Network Initiative, November 2016, 4. http://globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-the-ICT-Sector.pdf

63 "Extremist Content and the ICT Sector," 5.

64 Ibid.

65 "As White House and Tech Companies Meet on Terrorism, Privacy & Human Rights Organizations Demand Seat at Table."

66 Daphne Keller, Giancarlo Frosio, Luiz Fernando Marrey Moncau, and Jennifer Granick, "Intermediary Liability," Center for Internet and Society at Stanford Law School. http://cyberlaw.stanford.edu/focus-areas/intermediary-liability; Adam Holland, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster, "NOC Online Intermediaries Case Studies Series: Intermediarry Liability in the United States," Berkman Center for Internet and Society, February 18, 2015, 1. https://cyber.harvard.edu/is2015/sites/is2015/images/NOC_United_States_case_study.pdf

67 Anupam Chander, "Law and the Geography of Cyberspace," 6 W.I.P.O.J. 1 [2014] 99-106.

68 Jens-Henrik Jeppesen, "Strong Intermediary Liability Protection Focus of CDT response to European Commission's 'Platforms' Consultation," Center for Democracy and Technology, December 22, 2015. https://cdt.org/blog/strong-intermediary-liability-protection-focus-of-cdt-response-to-european-commissions-platforms-consultation

69 For example, the Counter Extremism Project has called upon social media companies to "grant trusted reporting status to government and groups like CEP to switfly identify and ensure the expeditious removal of extremists online." http://www.counterextremism.com/digital-disruption

70 "Submission to UN Special Rapporteur David Kaye: Study on Freedom of Expression and the Private Sector in the Digital Age," Ranking Digital Rights, January 29. 2016. https://rankingdigitalrights.org/wp-content/uploads/2016/02/RDR-Freedex-submission-Jan2016.pdf.

71 "Working Group 3 "Privacy and Transparency Online," Freedom Online Coalition, November 2015. https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf

72 Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010. https://www.treasury.gov/resource-center/sanctions/Documents/hr2194.pdf

73 Andi Wilson, Ross Schulman, Kevin Bankston, and Trey Herr, *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications*, New America's Open Technology Institute, July, 2016. https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf

74 Federal Register, Vol. 80, No. 97, Wednesday, May 20, 2015, Proposed Rules. https://www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015-11642.pdf

75 Morgan Marquis Boire, "Backdoors are Forever: Hacking Team and the Targeting of Dissent," Citizen Lab, October, 2012. https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent

76 Wilson et al., *Bugs in the System*.

77 Katie Bo Williams, "House Oversight Presses Kerry to Renegotiate Cyber Controls," *The Hill*, February 8, 2016. http://thehill.com/policy/cybersecurity/268641-house-oversight-presses-kerry-to-renegotiate-hacking-export-agreement

78 Wilson et al., *Bugs in the System*.

79 For an overview of the FOC working groups see https://www.freedomonlinecoalition.com/how-we-work/working-groups; For a description of Working Group 1, its mandate and membership see https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1.

80 Working Group 1: An Internet Free and Secure, Freedom Online Coalition. https://freeandsecure.online

81 Working Group 1: An Internet Free and Secure.

82 Danielle Kehl, Kevin Bankston, and Andi Wilson, "Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption," New America's Open Technology Institute, February 10, 2015, 13. http://static.newamerica.org/attachments/1866-oti-urges-un-human-rights-council-to-promote-the-benefits-of-strong-encryption/OTI_Crypto_Comments_UN.pdf

83 Danielle Kehl, "Encryption 101," *Slate*, February 25, 2016. http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html

84 Andy Greenberg, "Hacker Lexicon: What Is End-to-End Encryption?" *Wired*, November 25, 2014. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption

85 Stilgherrian, "Encrypting Data at Rest is Vital, But it's Just Not Happening," ZDNet, June 18, 2015. http://www.zdnet.com/article/encrypting-data-at-rest-is-vital-but-its-just-not-happening

86 Generally from "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," Human Rights Watch & The American Civil Liberties Union, July 2014, 24-61. https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf

87 Examples can be found in 'Regardless of Frontiers': The International Right to Freedom of Expression in the Digital Age," Center for Democracy & Technology, April 2011, 9. https://cdt.org/files/pdfs/CDT- Regardless_of_Frontiers_v0.5.pdf

88 Kehl, Bankston, and Wilson, "Comments to the UN Special Rapporteur."

89 "Freedom on the Net 2016: Bahrain."

90 "Freedom on the Net 2016: Columbia."

91 "Freedom on the Net 2016: Cuba."

92 "Freedom on the Net 2016: Pakistan."

93 Sarah Myers West, "The Crypto Wars Have Gone Global," Electronic Frontier Foundation, July 28, 2015. https://www.eff.org/deeplinks/2015/07/crypto-wars-have-gone-global

94 James Ball, Julian Borger and Glenn Greenwald, "Revealed: How U.S. and U.K. Spy Agencies Defeat Internet Privacy and Security," *Guardian*, September 6, 2013. www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

95 Craig Timberg and Barton Gellman, "NSA Paying U.S. Companies for Access to Communications Networks," *Washington Post*, August 29, 2013. https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html

96 Spencer Ackerman, "U.S. Tech Giants Knew of NSA Data Collection, Agency's Top Lawyer Insists," *Guardian*, March 19, 2014. https://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de

97 Craig Timberg and Greg Miller, "FBI Blasts Apple, Google for Locking Police Out of Phones," *Washington Post*, September 25, 2014. https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html

98 Ellen Nakashima, "Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks," *Washington Post*, February 16, 2016. https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

99 See Danielle Kehl, Kevin Bankston, Robyn Greene, and Robert Morgus, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity*, New America's Open Technology Institute, July 2014. https://na-production.s3.amazonaws.com/documents/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity.pdf

100 Cynthia M. Wong, "Internet at a Crossroads: How Government Surveillance Threatens How We Communicate," Human Rights Watch, 2015. https://www.hrw.org/world-report/2015/country-chapters/global-0

101 Wong, "Internet at a Crossroads."

102 Kenneth Roth, "The NSA's Global Threat to Free Speech," *New*

York Review of Books, November 18, 2013. http://www.nybooks.com/daily/2013/11/18/nsas-global-threat-free-speech

103 "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion, Frank LaRue," United Nations General Assembly Human Rights Council, A/HRC/23/40, April 17, 2013, 24-27. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

104 "Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy," 8.

105 Bill Marczak, John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender," Citizen Lab, August 24, 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae

106 Joseph Menn and Yeganeh Torbati, "Iranian Hackers Have Hacked Telegram—and it Could Spell Trouble for Activists and Journalists in the Country," *Business Insider*, August 2, 2016. http://www.businessinsider.com/r-exclusive-hackers-accessed-telegram-messaging-accounts-in-iran-researchers-2016-8

107 Tom Lowenthal, "Attacks on the Press 2015 Edition: Surveillance Forces Journalists to Think and Act Like Spies," Committee to Protect Journalists, April 2015. https://cpj.org/2015/04/attacks-on-the-press-surveillance-forces-journalists-to-think-act-like-spies.php

108 "FISA: 702 Collection," Lawfare. https://www.lawfareblog.com/topic/fisa-702-collection

109 John Napier Tye, "Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans," *Washington Post*, July 18, 2015. https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.6d652c58d78a

110 "FISA: 702 Collection."

111 Dia Kayyali, "The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why," Electronic Frontier Foundation, May 7, 2014. https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why

112 Tye, "Meet Executive Order 12333."

113 Mark Jaycox, "A Primer on Executive Order 12333: The Mass Surveillance Starlet," Electronic Frontier Foundation, June 2, 2014. https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet

114 Recommendations for Freedom Online, Adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

115 Ben Scott, "Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform," German Marshall Fund, November 5, 2015. http://www.gmfus.org/publications/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform

116 For the full set of surveillance-related recommendations, see p.[X]

117 "WG3 – Privacy and Transparency Online: Blog Series," Freedom Online Coalition. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-3/wg3-privacy-and-transparency-online-blog-series-2

118 Working Group 3 "Privacy and Transparency Online."

119 "MLAT: A Four-Letter Word in Need of Reform," Access Now, January 9, 2014. https://www.accessnow.org/mlat-a-four-letter-word-in-need-of-reform

120 Federal Judicial Center, "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges", 10. http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf

121 E.g., Treaty with Kazakhstan on Mutual Legal Assistance on Criminal Matters. https://www.congress.gov/treaty-document/114th-congress/11/document-text

122 U.S. Department of Justice, FY2015 Budget Request, https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

123 "Mutual Legal Assistance Treaties: FAQs," Access Now. https://www.mlat.info/faq

124 Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Telecommunications, 227. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

125 Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," Harvard Law School National Security Journal, January 28, 2015. http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age

126 Ellen Nakahsima and Andrea Peterson, "The British Want to Come to America—with Wiretap Orders and Search Warrants," *Washington Post*, February 4, 2016. https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html

127 Jennifer Daskal, "A New U.K.-U.S. Data Sharing Agreement: A Tremendous Opportunity, If Done Right", Just Security, February 8, 2016. https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity

128 "ACLU, Amnesty International USA, and HRW Letter on Opposing DOJ Proposal on Cross Border Data Sharing," American Civil Liberties Union, August 9, 2016. https://www.aclu.org/letter/aclu-amnesty-international-usa-and-hrw-letter-opposing-doj-proposal-cross-border-data-sharing

129 Ross Schulman and Greg Nojeim, "Foreign Governments,

Tech Companies, and Your Data: A Response to Jennifer Daskal and Andrew Woods," Just Security, August 30, 2016. https://www.justsecurity.org/32529/foreign-governments-tech-companies-data-response-jennifer-daskal-andrew-woods

130 "Cross-Border Law Enforcement Demands: Analysis of the U.S. Department of Justice's Proposed Bill," Center for Democracy and Technology, August 17, 2016. https://cdt.org/insight/cross-border-law-enforcement-demands-analysis-of-the-us-department-of-justices-proposed-bill-2; Schulman and Nojeim, "Foreign Governments, Tech Companies, and Your Data."

131 "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends," ICANN, October 1, 2016. https://www.icann.org/news/announcement-2016-10-01-en

132 "Coalition Statement in Support of Completing the IANA Transition," Center for Democracy and Technology and others, September 13, 2016. https://cdt.org/files/2016/09/IANA-transition-statement-final.pdf; "Civil Society Statement of Support for IANA Transition," Center for Democracy and Technology and others, May 24, 2016, https://cdt.org/files/2016/05/CSstatementonIANAtransitionMay2016.pdf

133 Stephen Shankland, "Why U.S. Internet Controls Became a Political Battlefield (FAQ)," CNet, September 16, 2016. https://www.cnet.com/news/why-is-us-giving-up-control-of-the-internet-dns-icann-domain-ted-cruz-faq; "Statements in Support of the IANA Stewardship Transition," ICANN, September 13, 2016, https://www.icann.org/en/system/files/files/iana-stewardship-support-statements-13sep16-en.pdf

134 See David G. Post and Danielle Kehl, *Controlling Internet Infrastructure: The "IANA Transition" and Why It Matters for the Future of the Internet, Part I*, New America's Open Technology Institute, April 2015, https://na-production.s3.amazonaws.com/documents/controlling-internet-infrastructure-part-i.pdf; David G. Post and Danielle Kehl, *Controlling Internet Infrastructure, Part II: The "IANA Transition" and ICANN Accountability*, New America's Open Technology Institute, September 2015, https://na-production.s3.amazonaws.com/documents/IANA_Paper_2_final.8594b4de27dd4ecf9be46d348f848cf1.pdf

135 "NTIA Finds IANA Stewardship Transition Proposal Meets Criteria to Complete Privatization," National Telecommunications and Information Administration, June 9, 2016, http://www.ntia.doc.gov/press-release/2016/iana-stewardship-transition-proposal-meets-criteria-complete-privatization and "CCWG-Accountability Supplemental Final Proposal on Work Stream 1 Recommendations." https://www.icann.org/en/system/files/files/ccwg-accountability-supp-proposal-work-stream-1-recs-23feb16-en.pdf

136 "ICANN Approves its Bylaws Including Commitment to Respect Human Rights Ahead of June Meeting in Helsinki," Article 19, June 23, 2016. https://www.article19.org/join-the-debate.php/244/view

137 "Launching Work Stream 2 in Helsinki," ICANN, June 23, 2016. https://www.icann.org/news/blog/launching-work-stream-2-in-helsinki

138 "Examining the Multistakeholder Plan for Transitioning the Internet Assigned Number Authority," Chris Calabrese's Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, May 24, 2016. https://cdt.org/files/2016/05/CDT-Calabrese-comments-May-24-Senate-IANA-hearing.pdf

139 Document: WSIS-05/PC-3/DT15 (Rev. 5)-E, World Summit on the Information Society, November 15, 2005. http://www.itu.int/net/wsis/docs2/pc3/working/dt15rev5.pdf

140 Wolfgang Kleinwächter, "The Start of a New Beginning: The Internet Governance Forum on its Road to 2025," Internet Society, April 1, 2016. https://www.internetsociety.org/blog/public-policy/2016/04/start-new-beginning-internet-governance-forum-its-road-2025

141 Constance Bommelaer De Leusse, "Reflections on a Successful IGF 2016", Internet Society, December 14, 2016, https://www.internetsociety.org/blog/public-policy/2016/12/reflections-successful-igf-2016

142 Shane Tews, "China Challenges Multi-Stakeholder Model of Internet Governance," Tech Policy Daily, December 23, 2015, http://www.techpolicydaily.com/technology/china-internet-governance; David Pandurksi, "China's Cyber-Diplomacy," China Media Project, December 21, 2015, http://cmp.hku.hk/2015/12/21/39527

143 Freedom Online Coalition.

144 Susan Morgan, "Clarifying Goals, Revitalizing Means: An Independent Evaluation of the Freedom Online Coalition," University of Pennsylvania Center for Global Communication Studies, May 2016. http://www.global.asc.upenn.edu/app/uploads/2016/05/FreedomOnlineCoalition_final_small-002.pdf

145 "Freedom on the Net 2016: France."; "Freedom on the Net 2016: United Kingdom."

146 Recommendations for Freedom Online, Adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition, https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

147 For an overview of the FOC working groups see https://www.freedomonlinecoalition.com/how-we-work/working-groups

148 "National Action Plans," Open Government Partnership. http://www.opengovpartnership.org/how-it-works/develop-a-national-action-plan

149 See: Extractive Industries Transparency Initiative. https://eiti.org

150 "FOC Working Group 3–Privacy and Transparency Online," Freedom Online Coalition. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-3; also see Ryan Budish and Liz Woolery, *Highlighting Best Practices in Transparency Reporting*, New America's Open Technology Institute, March 31, 2016, https://www.newamerica.org/oti/blog/highlighting-best-practices-in-transparency-reporting