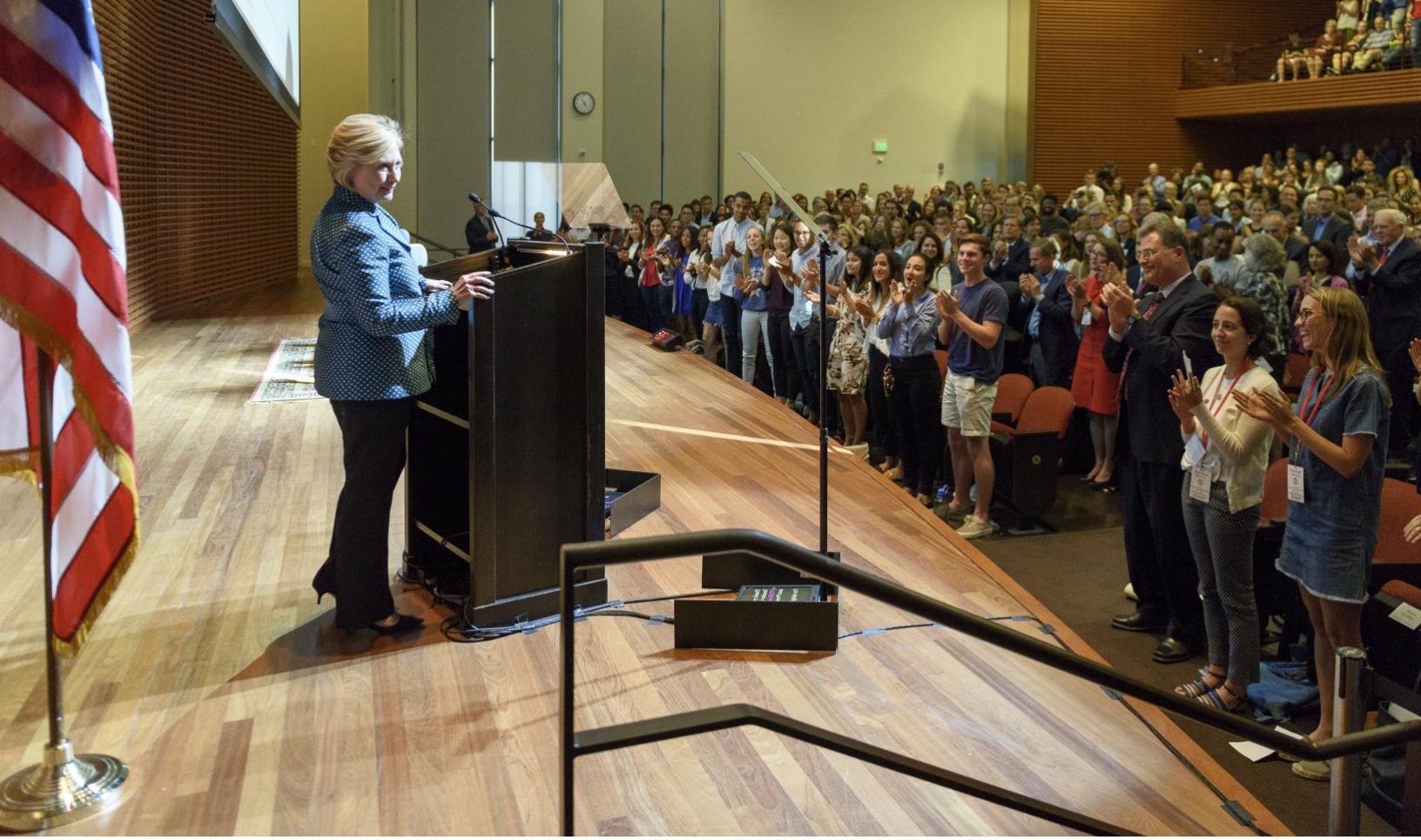


Launch of the

Global Digital Policy Incubator

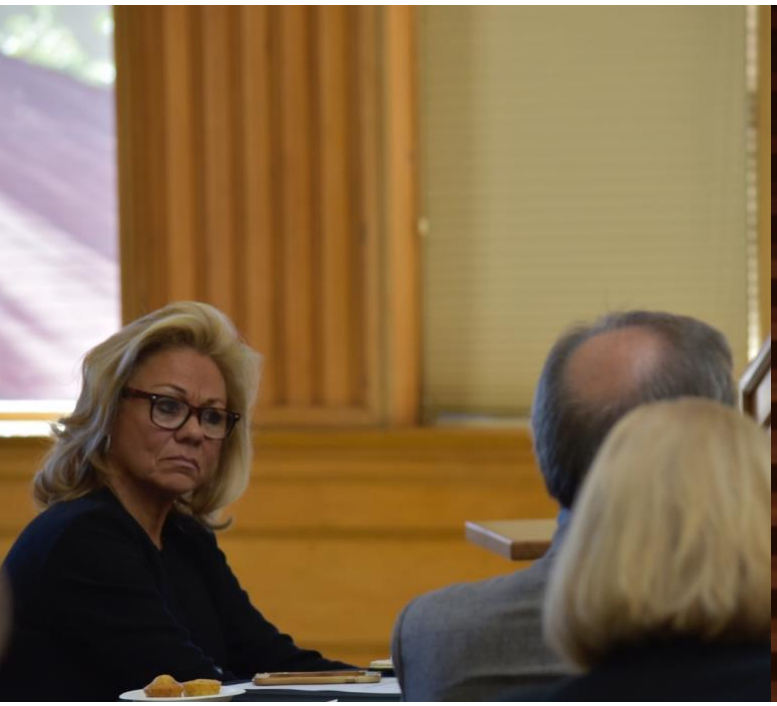
"Digital Technology and Democracy"

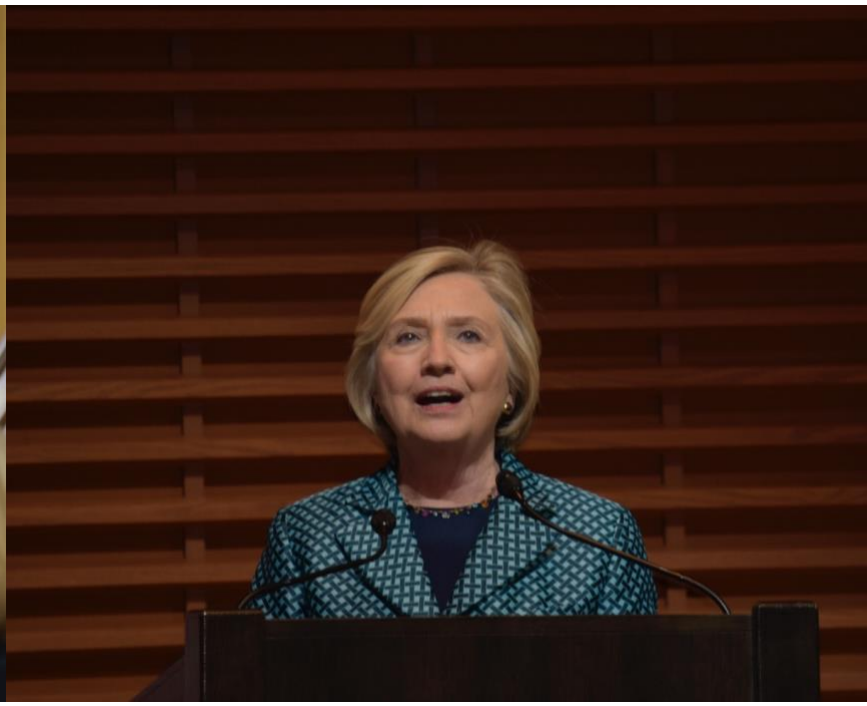
A summary of the Lessons Learned and Challenges ahead

Stanford University, October 6, 2017

CENTER FOR DEMOCRACY, DEVELOPMENT, AND THE RULE OF LAW | FREEMAN SPOGLI INSTITUTE FOR INTERNATINAL STUDIES

Table of Contents





Introduction

Global Digital Policy Incubator - Public Launch Event:

Democracy & Digital Technology

The Global Digital Policy Incubator (GDPi) at Stanford University's Center for Democracy, Development, and the Rule of Law, is a global, multi-stakeholder collaboration hub for development of norms and policies for our global, digital ecosystem. We bring together thought leaders and policy-makers to address conceptual and practical governance challenges that flow from digital technology, particularly when they bear on democracy and human rights. Our mission is to help the private sector, civil society and governments work together to craft effective policies that allow society to capitalize on the upside benefits of technology, while protecting against the downside risks.

On October 6, 2017, GDPi held our public launch event under the rubric of ***Democracy & Digital Technology***, where we focused on urgent governance challenges in the global digital Information ecosystem.

Our program started with an acknowledgment that we are at a pivotal moment for the future of democratic governance. To say that digital technology has disrupted society is now a cliché. The internet has become the infrastructure for our infrastructure and digital tools run through all sectors of society. Yet, we are only just starting to grasp the radical break we are facing with respect to the consequences of this digital transformation for our legal institutions and norms.

Policy-makers are struggling to deal with this dramatically changed global information ecosystem, where existing doctrine and regulatory approaches don't work. Digitization of information has led to the democratization of the means of distributing content, but this trend has also disrupted professional media which has traditionally played an important watchdog role in democracy. While digital tools have facilitated a dramatic expansion of access to information, ironically, democratization of production and distribution of content also has eroded the quality of discourse necessary to sustain democracy.

Governments responsible for protecting citizens against foreign attacks have been challenged by the instantaneous, cross-border reach of digitized disinformation, especially when weaponized to disrupt democratic processes. National and cyber security experts in democracies have not been adequately prepared to combat information operations or to defend against attacks on civic discourse. The increased efficacy of digital information

operations has changed how we think about protecting democratic discourse, and brought both conceptual confusion and fear to policy-makers. The bottom line is that globalized, digitized disinformation is undermining confidence in the legitimacy of democratic elections, and simultaneously eroding commitment to the value of free expression in democracies.

Furthermore, private sector digital platforms are playing significant new roles in "governing" the digital information ecosystem. Platform algorithms and micro-targeting tools are substantial factors in shaping access to information, and private sector terms of service and internal community guidelines dictate the parameters of free expression on digital platforms. While platforms depend upon the trust of their users, they are not democratically accountable to those users in the same way governments are accountable to citizens in a democracy. This fact raises conceptual questions about the responsibilities of digital platforms in democracy.

At the most fundamental level, a key set of questions we must answer stems from the fact that we do not know how to conceptualize our digital spaces: Are these public spaces or private spaces? Public resources or privately-owned infrastructure? If digital platforms function as the "public square" for civic discourse, who should make the rules about what speech should and should not be allowed on those platforms? How should international human rights law protections be incorporated by private sector platforms? How should platforms deal with national laws that are inconsistent with their own commitments to free expression or universal human rights principles? The answers to these conceptual questions will dictate some of the answers about who is responsible for governing those spaces, on what terms, and according to what values.

GDPI was created to help develop new norms and policies that reflect enduring democratic values and universal human rights. We see these values as sacrosanct and believe protect these values in the global digital ecosystem is possible and essential. But past articulations of these enduring values ---- as expressed in texts like the U.S. Bill of Rights and the Universal Declaration of Human Rights ---- as well as our legal doctrine about how to apply and implement those values, no longer meet the needs of our radically changed digitized ecosystem. A core challenge we face is figuring out how to hold onto our enduring values, but rearticulate them for our new context. To accomplish this task, we need to strike an optimal balance between continuity and change as it relates to past articulations of how to protect those values.

Our launch event program was divided into four segments:

The opening panel, entitled, ***When Freedom of Expression Conflicts with Democracy***, addressed tensions between our enduring value of free expression and the quality of discourse necessary to sustain democracy. An important foundation for this discussion was laid down by

Timothy Garton Ash, one of our panelists, as he shared insights from his book entitled, Free Speech: Ten Principles for a Connected World. The speed, scale, and extraterritorial reach of information in the digital realm means the effects of speech can be very different from speech in the pre-digital realm. Bots, troll farms, micro-targeting tools make "bad speech" different in kind – not just scale - from propaganda and hate speech of old. This panel focused on the need to figure out the implications of these different effects of digital information for our existing rules, and particularly on how we now must think about legitimate restrictions on speech in democracy, without undermining free expression.

This panel was moderated by Larry Diamond, Principle Investigator for the Global Digital Policy Incubator, Senior Fellow at the Hoover institution and the Freeman Spogli Institute for International Studies at Stanford. Panelists included: Timothy Garton Ash, Hoover Institution, Stanford, and Oxford University & Free Speech Debate; Frank Fukuyama, Director, Center for Democracy, Development and the Rule of Law at Stanford; Brittan Heller, Director of Technology & Society at the Anti-Defamation League; Ieva Kupce Ilves, cybersecurity expert and former Head of Cybersecurity Policy at the Ministry of Defense, Latvia; Justine Isola, Product Policy Manager at Facebook.

The second panel, entitled, ***When Information Becomes the Weapon***, addressed the growing national security threat from information operations and weaponization of information by foreign powers seeking to undermine democratic processes and discourse. This segment highlighted how difficult it has been for national security and cybersecurity experts to recognize the threats posed by information – which is supposed to be the lifeblood of democracy. Panelists discussed how to effectively combat the threat of information operations without eroding core values.

This panel was moderated by Michael McFaul, Director of the Freeman Spogli Institute for International Studies at Stanford, and former U.S. Ambassador to Russia. Panelists included: Toomas Ilves, former President Estonia; Mike Brown, Presidential innovation Fellow at DIUX and former CEO Symantec; Denis McDonough, White House Chief of Staff to President Obama and Senior Principal Markle Foundation; Nicole Wong, former U.S. Deputy CTO and former Google Vice President & Deputy General Counsel.

The third panel, entitled, ***Digital Platforms & Democratic Responsibility***, focused on emerging roles and responsibilities for private sector technology companies in "governing" and securing the digital information ecosystem. The panel addressed how difficult it has been to get a conceptual handle on how these platforms themselves should be governed, as their algorithms, terms of service and community guidelines shape public discourse in democracies.

This panel was moderated by Larry Kramer, President of the Hewlett Foundation. Panelists included: Juniper Downs, Global Head of Public Policy and Government Relations at YouTube;

Daphne Keller, Director Intermediary Liability at the Center Internet & Society at Stanford Law School; Andrew Mclaughlin, Co-founder, Higher Ground Labs, venture partner at Betaworks, and former U.S. Deputy CTO; Nick Pickles, Head of Public Policy and Government at Twitter; Mike Posner, Director, NYU Stern Center for Business & Human Rights and former U.S. Assistant Secretary of State for Democracy, Human Rights & Labor.

Finally, the fourth segment started with a **keynote speech by former U.S. Secretary of State Hillary Clinton on *Digital Technology, Diplomacy & Democratic Value*s**. Secretary Clinton described the cybersecurity threat landscape faced by democracies, and laid out her vision of the policy moves that will be necessary to protect democracies against digital disinformation. This speech was followed by conversation with GDPI Executive Director Eileen Donahoe, who served with Secretary Clinton during the Obama administration as former U.S. Ambassador to the UN Human Rights Council.

Overall, our program highlighted the reality that this is a peculiarly challenging juncture for policy-makers, specifically because of the growing perception that information and communication technology poses a threat to democracy. When conceptual confusion about how to govern, combines with fear about cyber threats running throughout society, even democratically inclined governments and well-intentioned private sector companies may get their policies wrong. This is the very real risk in our global digital information ecosystem.

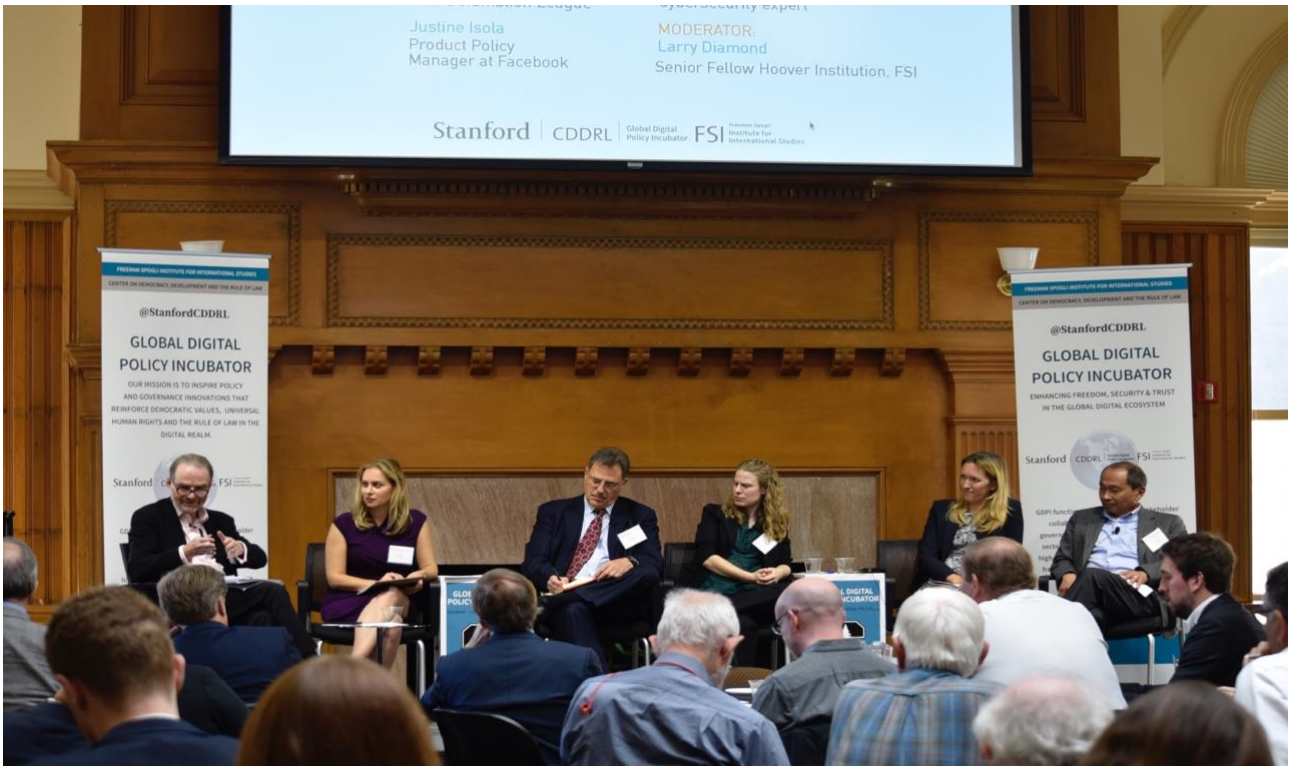
The key message we hope panelists and participants took away from this conference is that we all bear responsibility for helping craft policy to protect against digital threats to democracy. But as we engage is this urgent task, we must take care not to undermine universal human rights or democratic values in the name of protecting democracy.

Eileen Donahoe

Executive Director, Global Digital Policy Incubator

Panel 1: When Freedom of Expression Conflicts with Democracy

Enhancing the Quality of Discourse Necessary to Sustain Democracy



Quality and Veracity of Speech

Bots, "fake news" and other forms of unsourced or polarizing speech threaten the quality of political discourse in democracy. Anonymity, which is often essential to dissidents, plays a complex role.

Echo Chambers

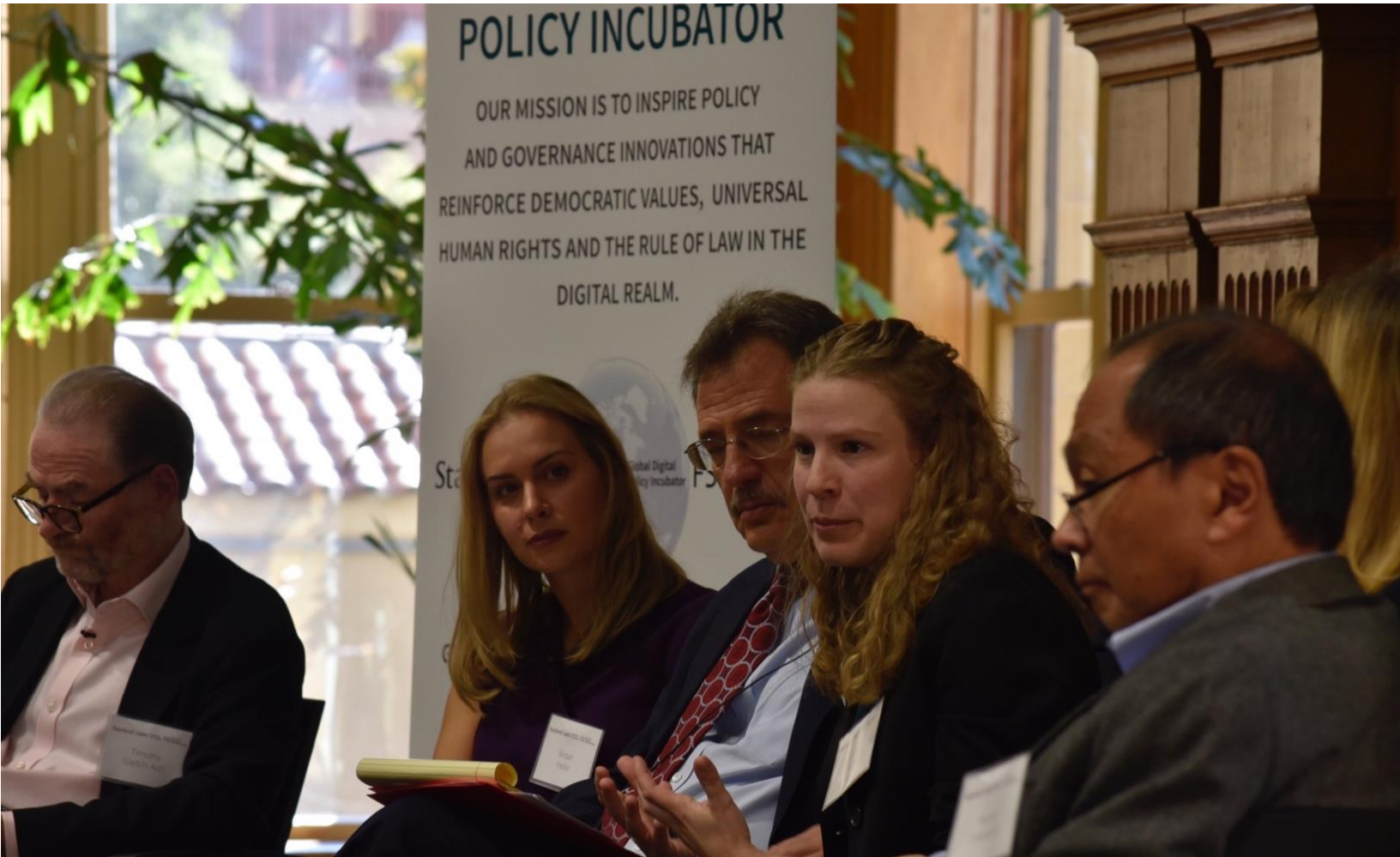
Echo Chambers reinforce tribal mentalities and contribute to polarization, but more research is needed to understand the impacts of social media platforms.

Building an Informed Citizenry

Access to information for an informed citizenry is the lifeblood of democracy, but disinformation and polarizing speech destroy civic engagement.

Timothy Garton Ash kicked off the inaugural panel, highlighting three foundational principles of democracies: freedom of expression, freedom of information, and the quality of democratic discourse. Garton Ash contends that in the new digital world, the third principle -- quality of democratic discourse -- is most in jeopardy. He highlighted 10 challenges to the quality of discourse in the digital era, which, while he indicated was not a comprehensive list, framed the multi-dimensional scope of the problem facing freedom of expression online. Panelists enumerated the various ways in which new technologies are eroding the quality of democratic political discourse. The informational and discursive dynamics on social media platforms quickly became the focal point of the discussion: including computational propaganda, bots, micro-targeting, echo chambers, and the instantaneous and unedited nature of the speech on digital platforms. Panelists also recognized that the same technological qualities that facilitate poor quality speech provide benefits as well. Panelists agreed that new tools and policies are needed to protect the quality of discourse and function as a check against unsourced or polarizing speech.

> *"If we who believe in both free speech and democracy are to argue against this dangerous development in Europe [referring to German Network Enforcement Act] … we have to have a much more credible story of what is actually being done about it by our government, by civil society, but crucially by the platforms."*



Ten Points to Frame Challenges to the Quality of Discourse in the Digital Age, by Timothy Garton Ash

1. ***Sheer Quantity*** *– Tackling the question, "how do you monitor billions of items of content coming up in 200 languages per day?"*
2. *If we believe the state has a legitimate role in regulation of certain online content, the* ***frontier hopping nature of the internet*** *makes that legitimate function more difficult.*
3. ***Democratic discourse requires robust civility****. There is nothing you can't talk about, but you talk about it in a civil way. The way the internet has developed, including the anonymity of the internet, produces a big challenge to robust civility.*
4. ***Impersonation*** *– You think you're being addressed by a fellow American voter, but in fact you're being addressed by a Russian bot.*
5. ***Disinformation and misinformation*** *– disinformation is false information maliciously disseminated for political reasons and misinformation is false information maliciously disseminated for other reasons. Research shows that false information is as likely to go viral as reliable information.*
6. ***Balance between virality and veracity*** *– Veracity is needed for a well-informed citizenry. If your algorithms privilege virality, you have a problem.*
7. *The* ***effect of echo chambers and filter bub****bles – we need much more research on this.*
8. ***Impact on established media*** *– the business model of most newspapers in the Western world has been blown out of the water. They are struggling for survival and so, privilege sensationalist content to generate a click stream.*
9. ***Tendency to monopoly****– hegemony by a handful of large companies poses a threat to media pluralism.*
10. ***Erosion of privacy*** *and the potential for mass surveillance.*

But what might these policy changes or regulation look like? Panelists cautioned against responses that jeopardize liberal democratic values, such as the legislative framework adopted by the German Bundestag in June 2017. The NetzDG or the German Network Enforcement Act imposes steep fines on private platforms if they fail to remove "clearly unlawful" speech, including hate speech within 24 hours. Several panelists mentioned self-regulation by private platform providers as the preferred solution, but they also acknowledged that companies like Facebook contend with an unprecedented scale. The immense quantity and reach of information posted on social networks complicates the burden of self-regulation.

Panelists also discussed non-regulatory methods for combatting the decline in the quality of political discourse. To address the problem of scale, panelists suggested the possibility of leveraging artificial intelligence to monitor content. As a response to polarizing speech, panelists suggested experimenting with new methods of assessing and relaying factual information. On the topic of anonymity, one panelist recommended allowing pseudonymous capabilities for human rights activists in dangerous environments to protect against reprisals, but otherwise requiring authenticated identities so

private companies could ensure there are actual human-beings behind accounts. Panelists reacted positively to Facebook's new feature designed to improve transparency on the context and source of posted content. The feature enables Facebook to empower democratic discourse and critical thinking without resorting to content removal.

The Bottom Line:

Liberal democracies, civil society, and private companies around the world must collaborate and support one another in addressing the deteriorating quality of political discourse in the digital space. The opening session of GDPI's launch event yielded a range of methods and ideas for stakeholders to consider as they work to address the tensions between free expression and democratic engagement.

Panelists:

Timothy Garton Ash
Hoover Institution, Oxford University & Free Speech Debate

Francis Fukuyama
Director of Stanford Center for Democracy, Development and the Rule of Law

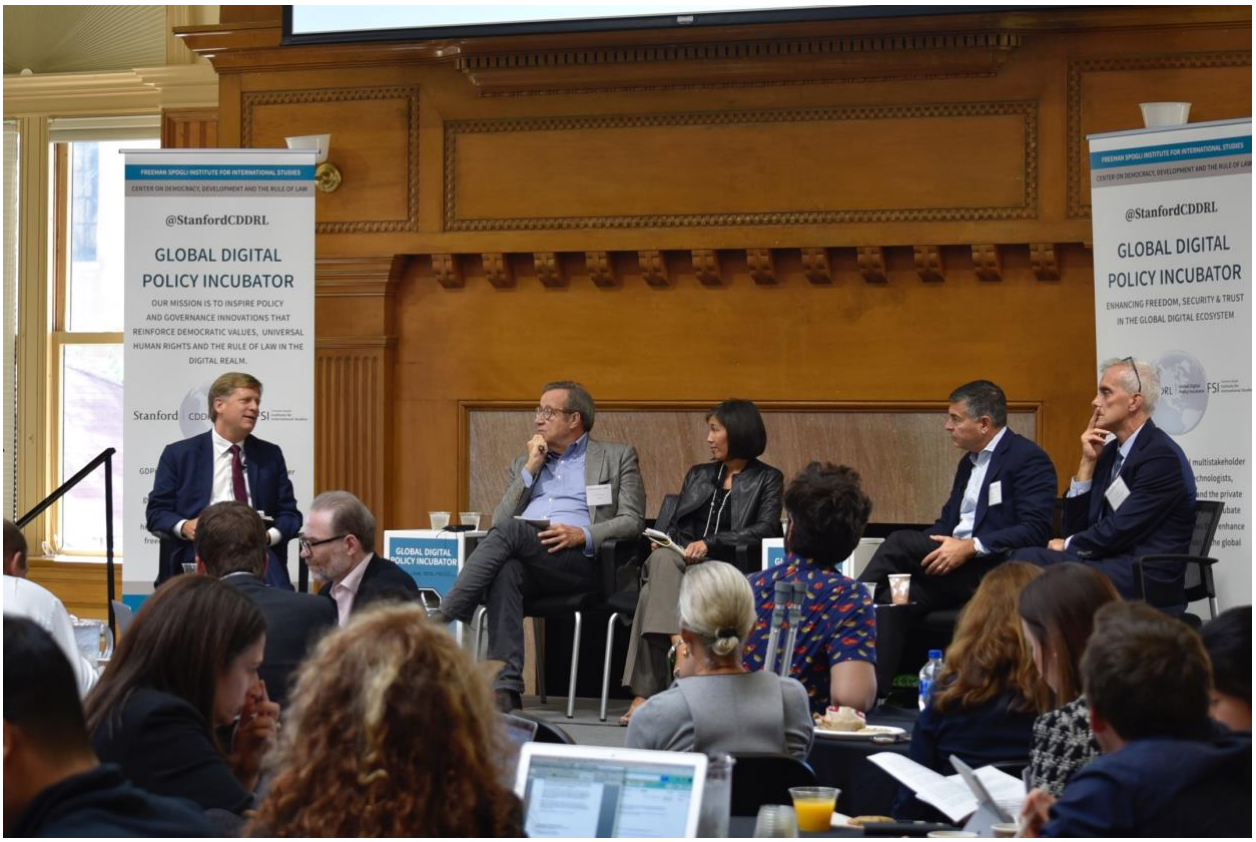
Brittan Heller
Director of Technology & Society Anti-Defamation League

Ieva Kupce Ilves
Cybersecurity Expert, Former Head of Cybersecurity Policy, MoD Latvia

Justine Isola
Product Policy Manager, Facebook

Panel 2: When information becomes the weapon

Expanding notions of national security in the digital context



Asymmetry in Information Warfare

Democratic governments need to develop a range of appropriate, effective responses to informational attacks, and have a variety of tools at their disposal to respond to asymmetrical threats.

New Cyber Norms

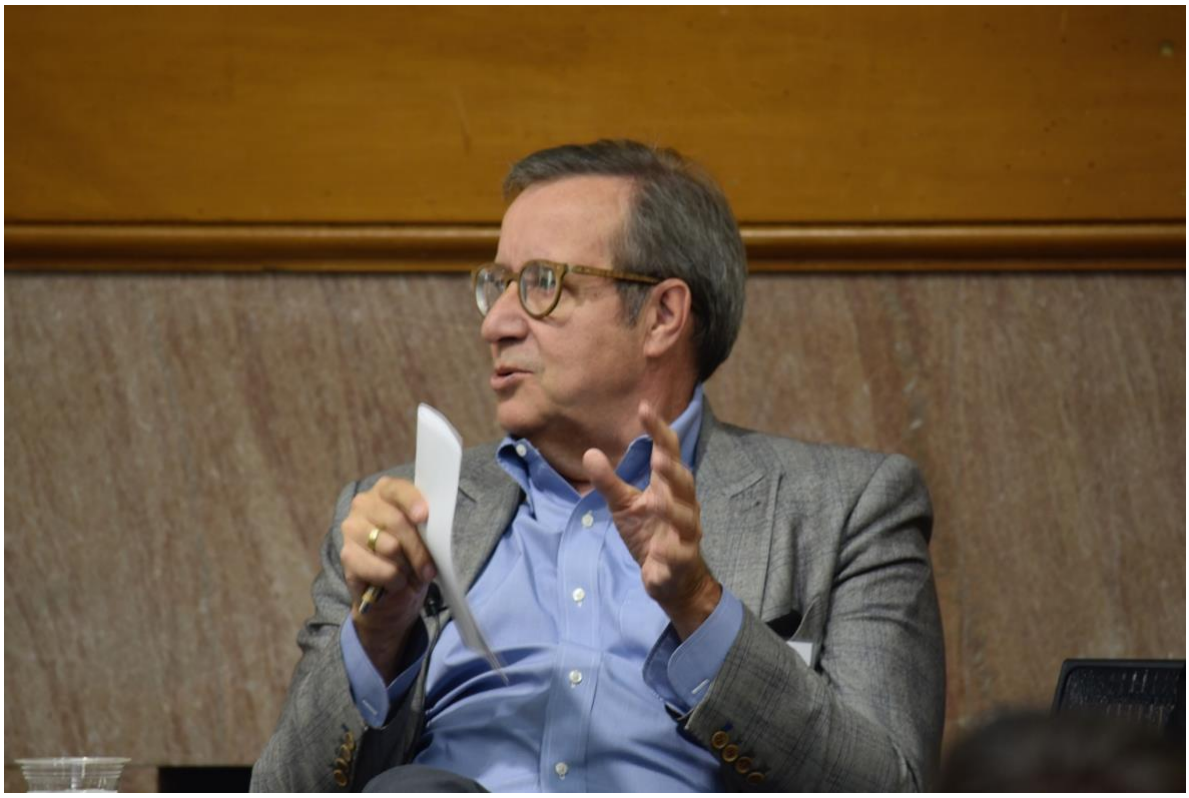
In addition to technical solutions, new norms for cyber offense and defense must be developed. Norms of civil discourse and media standards for reporting on doxing of private information need to change.

Role of the Private Sector and Government

Private companies cannot defend against cyber threats alone. Democratic governments should set norms for an offensive response to informational attacks.

This panel focused on the problem posed by "information operations" - foreign governments' use of digital technology to spread propaganda, as well as defensive and offensive tactics to combat this strain of cyber threat. While the panelists agreed on the nature and gravity of the problem, they debated whether or not technology was the primary cause (and therefore the primary solution) for the increased diffusion of foreign sponsored propaganda. Some panelists contended that getting rid of bots is not enough. Deep partisan divides and a distrust of political institutions primed U.S. citizens for the reception of disinformation in the lead up to the 2016 U.S. presidential election. As one panelist noted, Americans were "weaponized against themselves". Fighting against digital information attacks will require not only changing technology, but also changing norms around civil discourse and the media.

"The media has let us down in part because they aren't functioning as gatekeepers on big news. In a lot of ways, they're chasing that shiny ball of sensationalism. . . which just serves to amplify it."



The panel agreed that government must assume a larger role in combating this threat, but not on what the government's role should be. Government jurisdiction in the digital space is blurry. As one panelist noted, Americans call the police after a robbery, but they call the IT department after an email hack. But because most of the larger attacks observed in the digital realm are

state sponsored, citizens must look to the government to respond to cyberattacks. The hard question raised was how democratic governments can respond effectively without eroding their own norms. Some panelists advocated for allowing "hack-backs" by both US government agencies and private companies. Others called for increased cybersecurity standards (such as encryption requirements and two-factor authentication). The idea of a digital "Geneva Convention" to protect civilians from hacks in peacetime was floated, but panelists quickly noted that the countries most likely to use cyberattacks against civilians would not be likely to participate. Russia and China would not necessarily comply, while democracies would feel constrained from attacking with the same methods employed against them.

> *"We are in an asymmetrical war. . . Liberal democracy cannot use these [same] tools on an authoritarian regime that an authoritarian regime can use against liberal democracy."*

The Bottom Line:

The panel acknowledged that the biggest challenge with information warfare is its asymmetric quality: so many attackers and attack vectors, combined with requirement of legitimate and proportional responses by democratic governments. Yet, liberal democracies have many legitimate tools at their disposal to respond to authoritarian regimes targeting their citizens– visa restrictions, money laundering rules, and sanctions. In this new digital context, improvements in attribution and identification of who is behind the disinformation published online can be an important line of defense. Resilience to withstand an attack may be a more effective deterrent than any counter-attack.

Panelists:

Toomas Ilves
Former President of Estonia

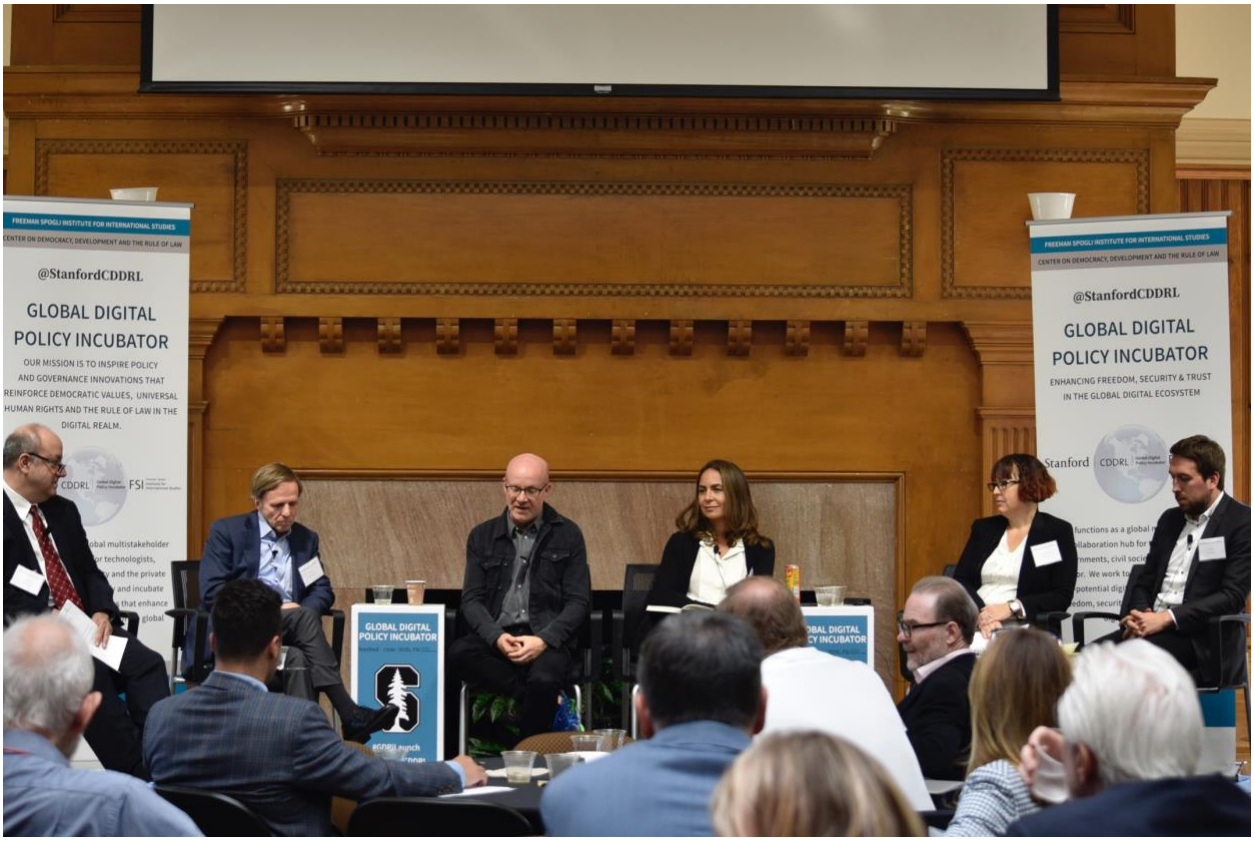
Nicole Wong
Former US Deputy Chief Technology Officer

Mike Brown
Former CEO, Symantec

Dennis McDonough
Former White House Chief of Staff to Obama

Panel 3: Digital Platforms & Democratic Responsibility

Emerging Private Sector Roles in Protecting Freedom and Security



Responsibility for combatting misinformation and disinformation

We don't have a definition for "fake news." Who should be the arbiter for identifying and removing "fake" content?

Costs of over-censorship

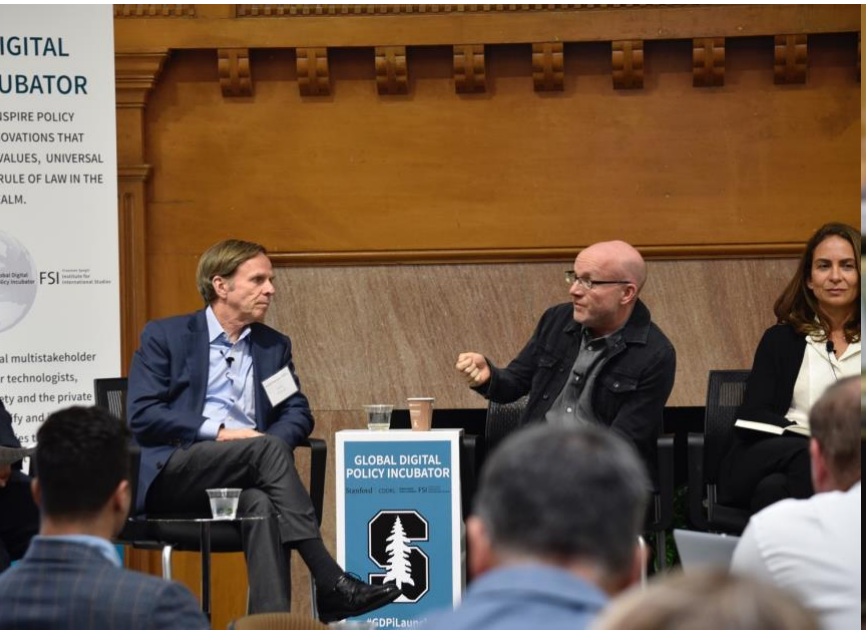
A balance must be struck in regulating content: We cannot allow regulation to eclipse the positive benefits for expression that digital platforms provide.

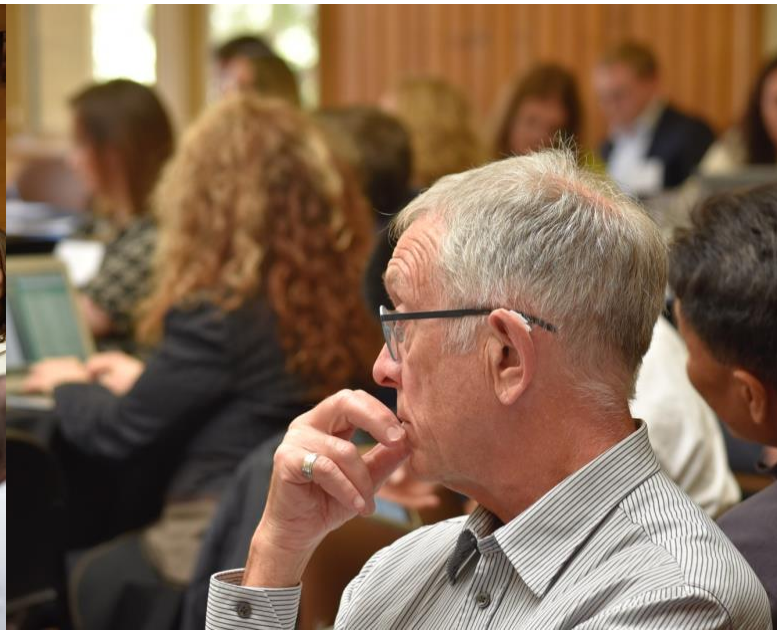
Platform norms on free expression

How should private sector TOS and community guidelines relate to free expression norms, like the First Amendment or Article 19 of the International Covenant on Civil and Political rights (ICCPR)?

Speakers on this panel discussed private sector responsibilities in regulating speech online. The panel was divided on the level of responsibility for private companies in combatting misinformation, disinformation and hate speech. Panelists representing large internet platforms, such as Twitter and YouTube, discussed the role internet platform algorithms play in curating and surfacing authoritative and relevant content. They also discussed platform responses to government takedown requests and platform transparency with respect to those requests. Platform self-regulation through community guidelines often extend beyond what the law requires and raise new conceptual challenges for the protection of free expression. Platform representatives also stressed the risks of assigning increased "state-like" responsibility to private companies to monitor speech. For example, if governments ask the private sector to prioritize veracity over virality, the delay in the publication of speech could have profound implications for the free speech of civil society actors, such as the speed at which human rights violations can be reported to the global community. With increased responsibility, platforms are also likely to over-censor to protect themselves against liability. Other panelists took an opposing view, stressing the active and prominent role that platforms already play in the curation of speech and information online. Panelists from academia, civil society, and government felt strongly that private sector companies have not taken enough of a proactive stance in fighting misinformation and disinformation on their platforms. Panelists also mentioned that paid advertising on platforms should be subject to more stringent rules, prompting a discussion of the need for stronger content regulation in the campaign advertisement space.

> *"The concerns that everyone has about the power that these platforms have over individuals and society when looking through the lens of risk -- is exactly why we care about the First Amendment when looking through the lens of benefit."*





The panel ended with a discussion of the First Amendment of the U.S. constitution and global norms of free expression. A question was raised about whether democracies need to re-evaluate the traditional view of freedom of speech in the digital space. If governments increase regulation and push private companies to remove particular types of speech on their platforms, how do platforms ensure they are not facilitating authoritarian government objectives to silence political dissent? Free expression principles, as expressed in the First Amendment of the U.S. Constitution and Article 19 of the ICCPR do not rest on the premise that there is no bad speech. They rest on the idea that there are no good rule-makers. The hard question is who regulates speech and how should they do it? While the panelists reached no consensus on how to regulate online speech, the discussion framed the challenges and opportunities for civil society, government, and private sector companies as they seek viable policy options and tools.

"The protection of free speech under 20th century norms in new technology frameworks is threatening democracy globally and in the United States. All rights rest on both explicit and implicit policy balances. There is an implicit cost benefit analysis that we take for granted…"

Panelists:

Juniper Downs
Global Head of Public Policy and Government Relations, YouTube

Daphne Keller
Director of Intermediary Liability, Stanford Center for Internet and

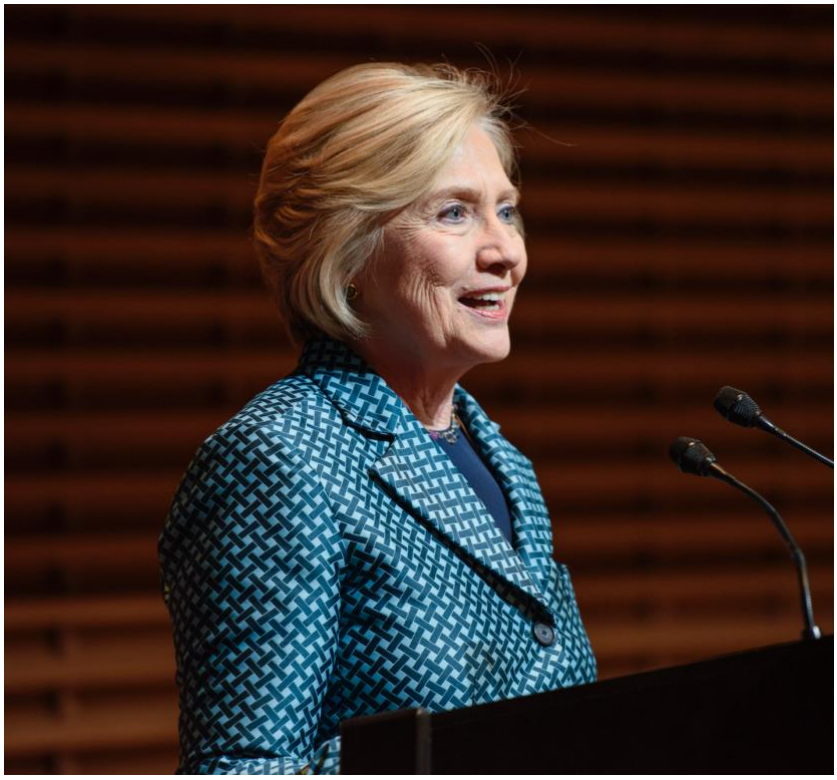
Andrew McLaughlin
Higher Ground Labs, Betaworks, Former Dep. U.S. CTO

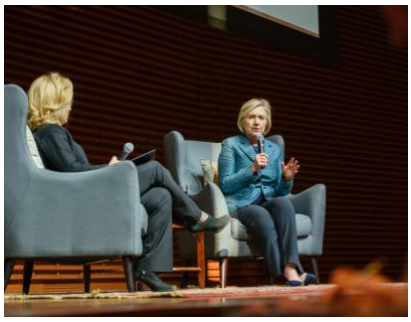
Nick Pickles
Senior Public Policy Manager, Twitter

Mike Posner
Director, NYU Stern Center for Business & Human Rights, Former U.S. Assistant Secretary of State

Keynote: Digital Technology, Diplomacy, and Democratic Values

A conversation with Eileen Donahoe and Hillary Rodham Clinton





"This is a new kind of cold war – and it's just getting started."

Secretary Clinton's keynote discussed the future of democracy amid the challenges posed by technology, propaganda, terrorism, and espionage. While acknowledging the immense good that digital technology has produced for democracy around the world, Secretary Clinton cautioned that this same technology can be used to harm society – as evidenced by the 2016 election. Clinton focused on the information war waged on the U.S. by Russia during the election, but she also warned that the threat to democracy extends beyond American borders. The Russian government has used digital technology to sow seeds of division in Germany, France and Spain, and will only continue to do so, targeting democracies worldwide. She concluded with five recommendations to protect American democracy from emerging digital threats:

Get Serious About Cybersecurity:

The government and private sector need to work together to prioritize the protection of American networks and infrastructure. We had our "wake up call"! We need to treat a cyber-attack by a foreign state as an act of war. Government intelligence agencies should develop an offensive strategy and share any information they receive quickly with utilities, private corporations, and other who need that information to quickly act to protect our nation.

"We all have the ability to break out of our echo chambers and engage with people who don't agree with us politically. . . even if our outreach is rebuffed, it's worth it to keep trying. We know Putin and the Russians are doing everything they can to divide us. Why would we help them along?"

Get Tough on Putin

No foreign power has attacked the United States with so few consequences in modern history. While Congress passed sanctions against Russia, they have yet to be implemented. The US government needs to react strongly so that Putin "feels steel" when he probes. We also need to work with NATO to strengthen their cyber-attack resources.

Close Election Law Loopholes

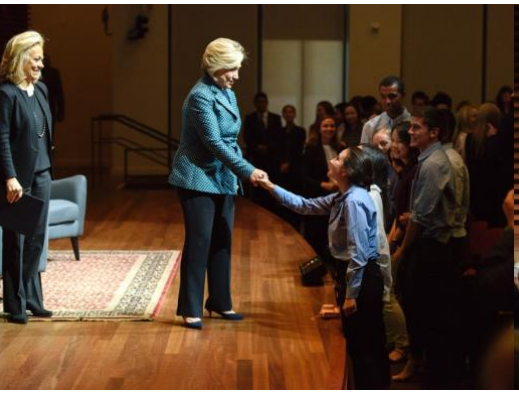
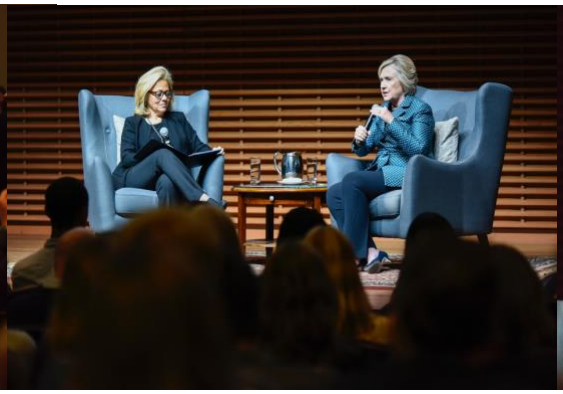
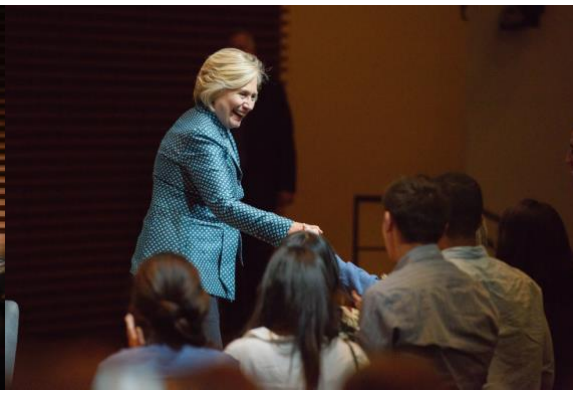
Elections are won and lost online, so why do governments still use analog regulations? All political advertising online should adhere to the same standard as television ads. Foreign entities should be banned from issue advertising. International governments are already prohibited from contributing to political campaigns, and should not be allowed to support a candidate through advertising either.

Complete Public Accounting of What Happened in 2016:

In addition to the ongoing special investigation, the government should create an independent commission with subpoena power to conduct a robust investigation of the 2016 election. Said commission should present a report to the public, complete with recommendations to guide future policy. Additionally, the government must demand a full account from Facebook, Twitter, Google, and other digital platforms. Americans must depend on transparency and accountability from these powerful companies.

Fight Back Against the Assault on Truth and Reason:

America must launch massive education campaign against fake news focused on teaching young learners to be critical thinkers who value facts and evidence. The mainstream media also has a role to play in debunking lies. The partisan divisions that allowed digital propaganda to flourish can be countered by citizens engaging with fellow Americans with whom they may not agree politically. Americans don't have to agree, but they do need to learn to have conversations with one other based on facts.

Q&A

Excerpts from the conversation between Eileen Donahoe and Secretary Clinton, plus audience questions

On the decline of truth:

Q: What happened to our belief in facts, and what can we do to restore our cultural commitment to truth and factual analysis as the basis of our political discourse and policy?

A: "The body politic has to have a strong immune system just like the physical body. And our national immune system has been worn down over the last decade . . . there has become an industry of fabrication for the purpose of gaining [commercial, partisan, and ideological] advantage and it has battered the immune system of our body politic. And it has been accelerated and made all pervasive by the advances in technology."

"If we don't start in our own home and we don't have better interrogation in the media of people wo are making outrageous claims, it's really hard to protect ourselves against the onslaught coming from the outside by Russians or anybody else."

On the media reporting:

Q: How did the mainstream media fail to see that their reporting on John Podesta's doxed email amounted to unwitting participation in an act of political sabotage? And what can we do about the ethos around doxing?

A: "People just think if something looks like its secretive it's somehow got to be more authentic"

"It's not only the deliberate effort to plant false stories, it's [also] a great distraction. Don't let people look at what's really going on and what will have long-term consequences for our country, let's keep everybody chasing rabbits over here. [We need to] ask the press to engage in a serious conversation [about this]."

On the impact of future technology:

Q: What do you hope for from the students here today, as we try to tackle the ethical challenges that flow from technology - ranging from online hate speech, to disinformation, to the implications of AI for democratic governance? What would you ask of the students here?

A: "I would hope and maybe implore you to keep in mind the kind of value questions and ethical considerations that have to now be part of the debate about the consequences of technological advances. There's so many reasons to be optimistic and confident. . . but we are getting to the point where a lot of the changes on the horizon will have far reaching economic, social, and political consequences."

"Somebody has to help organize that debate; to be a referee, and umpire. Try to get the smart people who are on the cutting edge of technology to stop long enough and listen to what the consequences might be"

On social media and gender dynamics:

Q: What can we do to awaken people to the connection between gender dynamics on social media and how it affects political engagement and the democratic process for everyone?

A: "The first step is to talk about it. If you don't talk about it or if you try and talk about it and you're immediately shut down, we're never going to change the attitudes and the norms that still impact women and girls and their own ambitions and aspirations."

"The attacks [on women online] are vile. The things that are said are just horrific. And let me say, this doesn't just happen from the right. It happens from the left [as well]. [They] go after women from the left and right. Why? Because we have opinions? Because we're pushy? Because we want to be President?"

On individual responsibility:

Q: What can we do as individuals to improve the quality of civic engagement in our country and halt the spread of misinformation and polarizing discourse?

A: "It is so important that young people decide . . . that you're going to vote every time you get a chance to vote."

"A lot of what is online now is just insult after insult. . . It's not discourse. . . don't come with profanity-laden arguments. Come with facts. Step up and tell us why you believe something, rather than just pretending your position is better than mine without being able to defend it."

On government regulation:

Q: How do you think about the roles and responsibilities of private sector platforms, governments, and citizens to address digital propaganda and hate speech?

A: "I think there is a lot the companies can do themselves. More accountability and checking on the source of material [online]."

"I think we have to have an honest debate with the companies, with ourselves, to figure out what we need to do. . . People have seen in recent years what happened with Bosnia or Rwanda, where hate speech wasn't online, it was good, old-fashioned radio and TV. But imagine how much more powerful it would be if it were online."

On hope for the future:

Q: What makes you hopeful now about civic engagement in the digital realm?

A: "New, young, vigorous grassroots groups engaged in civic activity, political activity, recruiting candidates. . . that kind of energy . . .gives me reason to be hopeful. . . I find it hard to believe that the level of political behavior that we're currently seeing won't be self-corrective."

Close:

In closing, I want to bring back a memory for you. In your book you talk about the people who took care of hair and make-up so it wasn't a distraction on the campaign trail. So I have this memory of when I was in Geneva that connects your global leadership on human rights to digital technology and your hair.

It was International Human Rights Day, 2011, and you came to Geneva to give this groundbreaking speech on LGBT rights. And it may be hard for people here in Silicon Valley to appreciate the extent to which this subject was completely taboo in the international community at the time just 5-6 years ago. This was a time that LGBT activists were literally being hung from trees and being murdered for their advocacy. So you came to Geneva to break that taboo and use your political capital in front of the international community as a champion for human rights and LGBT rights.

Here's the hair part - on this trip, Huma was about to give birth so she couldn't travel to Geneva, and so nobody had made arrangements for your hair. So you were about to go out there and give this big speech, and you came up to me, you grabbed me by the shoulders, you looked me in the eye, and you said "Eileen, I need your hairdresser."

So we got that arranged the next morning.

But you were literally on your way out to give that speech in front of thousands of people. It was live streamed and Twitter just lit up. Your message spread globally and there was an instantaneous buzz. You single handledly change the global conversation about LGBT rights. But half the tweets were saying, “What’s up with her hair?”

And so for me, I think of this story as a kind of a bonding story for all women in the public realm, and I hope it provides a humorous reminder of what global leadership actually looks like.

Annex

Speaker Reflections

We asked our speakers to provide us with some closing thoughts. Here's what they had to say:

Thoughts on Social Media and Free Speech

By Larry Kramer

I'll talk about free speech rather than "the First Amendment" because I think it matters that the First Amendment applies only to government, and we should have different expectations for government and private actors. When people at Facebook or Twitter or Google say they cannot do this or that, or must do this or that, because of the First Amendment, they are implicitly importing a standard that may be inappropriately stringent as applied to them. The issue more properly understood is how, as a cultural and social matter, they—as private actors—should think about the value of free speech in society (not to mention whether and how speech commitments should affect their bottom line).

It's a mundane point, though I do wish people would get it right. The more significant point is the fundamental way in which the 20th century debate over free speech needs to be rethought. Here's why: legal norms are shaped by both explicit and implicit ideas and assumptions. The explicit ones are the policy justifications that we argue about, reflecting the cost/benefit analysis we see the right as embodying (because all rights have limits and the limits of all rights reflect a balancing of costs and benefits): "The purpose of this right is X, and this interpretation better advances that purpose." Or "No, the right does not require accepting cost Y, therefore this interpretation is better." As applied to speech, it's why you really can't yell "fire" in a crowded theater and why it is alright for government to require time, place, and manner restrictions on the use of public spaces.

"Legal norms are shaped by both explicit and implicit ideas and assumptions . . . So, if they change, we cannot simply continue to engage in the same arguments we did before. We need to rethink the whole balance."

The vast bulk of argument about rights and their scope is of this ilk. But rights also reflect *implicit* assumptions that shape how we think about and understand their costs and benefits, and these implicit assumptions are typically invisible because they reflect given aspects of our world—things that affect the scope of the right in ways we take for granted, without even realizing it. Unseen, they nevertheless profoundly influence the law. So if they change, we cannot simply continue to engage in the same arguments we did before. We need to rethink the whole balance.

Let me illustrate with a couple of analogies:

(1) **Tort law.** In the 19th century, we developed a law for accidents on the highway. It had the familiar doctrines of negligence, proximate cause, assumption of risk, etc.—all articulated in particular ways that fit the problem of accidents on the highway and balanced our sense of who (driver, victim, manufacturer) should bear what costs and under what circumstances. But accidents on the highway were relatively rare and injuries were seldom fatal. Why? Because transportation was by horse or horse and carriage, meaning there were never that many people on the road, they could not go especially fast, and so on.

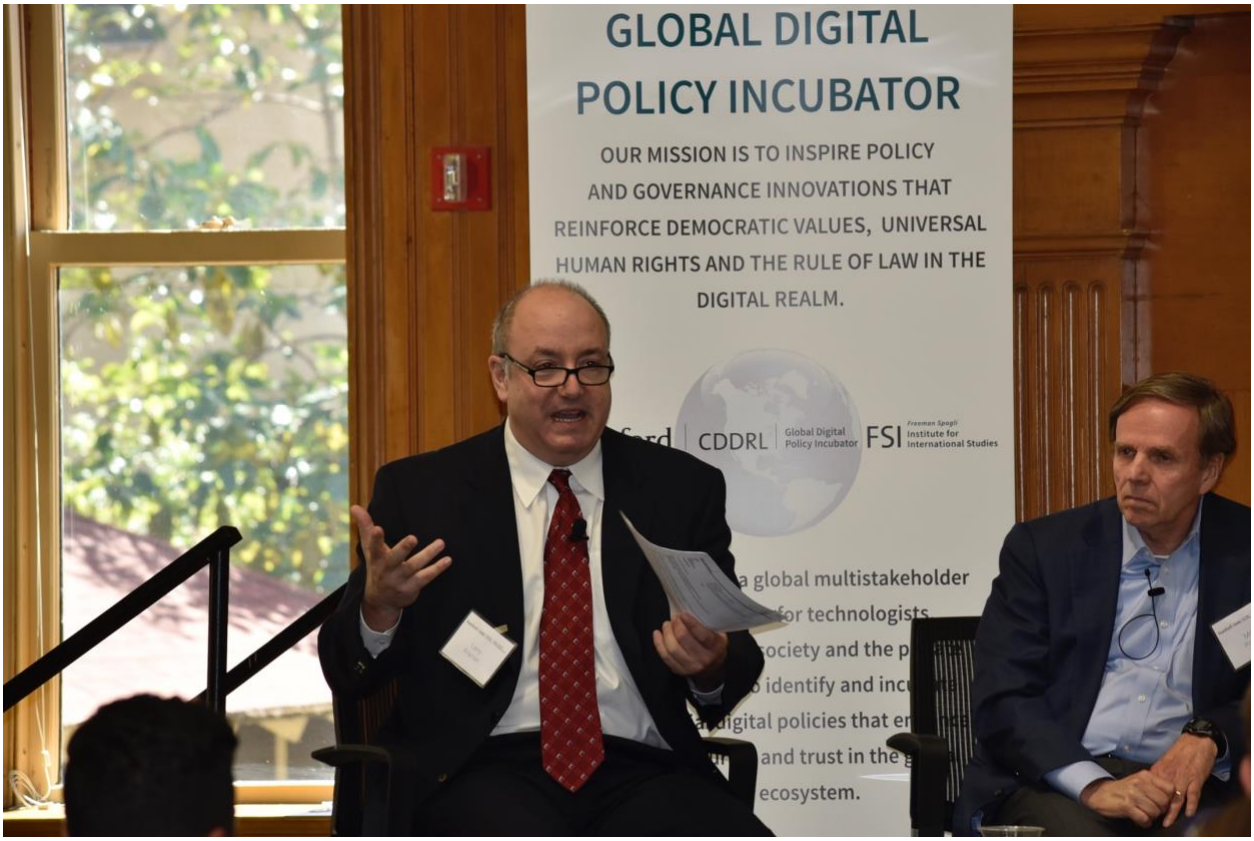
Then along comes the car, and it fundamentally transforms the circumstances of highway travel in ways no one could possibly have imagined when they developed this law in the first place. In such circumstances, one can't simply take the 19th century doctrines and continue to apply them in the same way, as if existing precedents provide appropriate analogies. The shift from horses to cars fundamentally transformed the world in which tort law is situated. Instead, we needed to rethink tort law to conform to a new world, which is precisely what we did.

(2) **Copyright.** Changes like this—changes that transform the implicit assumptions on which the legal cost/benefit analysis rests—are frequently driven by new technologies, which reshape possibilities in ways that were not and could not have been foreseen earlier. Copyright is another example. The modern law of copyright developed in the early 20th century. As a formal matter, it provided very strong protection. Subject only to a limited fair use exception, copyright was formally absolute, meaning no one could use my intellectual property without first obtaining my permission. In practice, of course, some piracy occurred. But its extent was limited by the practicalities of existing technology. On the one hand, there

"Changes like this – changes that transform the implicit assumptions on which the legal cost/benefit analysis rests – are frequently driven by new technologies, which reshape possibilities in ways that were not and could not have been foreseen earlier."

was only so much you could do to exploit my copyright without attracting my attention; on the other hand, so long as you confined yourself to that small amount, you got away with it. This limited capacity to use copyrighted materials without permission provided a useful safety valve, enabling small but essential uses.

Then everything went online, and two things happened: (1) you could now pirate on a mass scale, much greater than anything you could have done when we were just talking cassette tapes and such (think Napster); (2) I could now prevent all pirating altogether, even single uses, by employing technology that prevents anyone and everyone from making copies. In a classic example of failing to understand, Congress initially ignored the importance of the new technology and simply applied the explicit part of the 20th century legal regime, which said the copyright owner has an absolute right. They gave us the Digital Millennium Copyright Act, which then created massive pressures for much greater levels of piracy. We still haven't sorted it out.



(3) **Privacy.** The current debate over privacy is similar. The 20th century balance of costs and benefits that underlies our inherited privacy notions are fundamentally upset by the Internet. We can't just apply Brandeis's arguments in this world, can't employ the classic "the purpose is X, therefore this interpretation applies," because new technologies have transformed both the

costs and the benefits of that notion of privacy. Technology creates much greater threats, but it also creates much greater potential benefits. By way of example, I had an argument with a Stanford engineer over his right to privacy respecting his genetic information. He believed it should be absolute. I asked him if he would still take that position if I could show him that getting the genetic information of everyone in America would enable me to cure cancer. He said yes—even in that case, even if it would enable me to cure death itself, his right is absolute. It wouldn't be enough to guarantee anonymity. It is, he said, "his" genetic information, and he should be able to keep it private if he wants. I think that's ludicrous, though it does follow from 20th century legal norms. But those norms were developed in a world in which neither the kind of privacy concerns we now face nor the potential benefits from abrogating them were even imaginable.

The same kind of analysis applies if we think about free speech and social media/Internet. Actually, it is true even if we think more pointedly about the First Amendment and what we might want to allow government to do.

Imagine it is 1964, and someone thinks they have a great story about how LBJ is running a child trafficking ring out of a D.C. pizza parlor. He wants to get this important story out. What can he do? He can go to the New York Times or CBS and tell them about it, but they'll just show him the door. Not because they only run stories from their own reporters: they run things from wire services and accept stories from freelance investigative reporters. But they curate the news they run, as do all the major papers and radio and TV stations. They will refuse to run this sort of deranged inanity, as they would likewise refuse to run a story that wasn't insane but was plainly propaganda (for instance, a story built on a true fact but distorted and embedded in an overtly emotional appeal to hatred).

Our friend can self-publish: there is free speech, after all. But he will only be able to reach a tiny audience, because he will not have the resources or technological capacity to do more. There are some extremist outlets: he might try the John Birch Society or the Communist Party, both of which have their own papers and might run his story. This would reach more people, though only those who go looking specifically for what the Communists or white supremacists have to say, still a very small group. In short, the technology of news distribution, combined with the curatorial practices of the major news producers—who are, of course, also the major news distributors—ensured that most Americans were exposed only to fairly responsible news and information.

Then along comes the Internet, followed by social media, and everything changes. The new technology enables our friend very cheaply to produce this story himself, at a fairly high level of quality. And particularly once social media are around, the same technology enables him to reach a mass audience of people who might not otherwise have encountered his ludicrous story or his cleverly crafted propaganda.

"The rise of social media, and the increasing tendency of people to get their news this way, splits the news production function . . . from the news distribution function (now done through the Internet platforms). But unlike the old mainstream outlets, which curated as part of their production function, the new social media won't curate at all."

The former change (easy to produce) is purely a matter of technology. The latter (easy to distribute) is a matter of a change in the way news is distributed that grows out of the technology. The rise of social media, and the increasing tendency of people to get their news this way, splits the news production function (still done by the Times, CBS, and other major mainstream media) from the news distribution function (now done through Internet platforms). But unlike the old mainstream outlets, which curated as part of their production function, the new social media won't curate at all. Suddenly millions of Americans who, in the old days, would not have been exposed to a certain kind of misinformation/disinformation are getting inundated. Worse, precisely because it is so much easier and cheaper to produce and distribute, the amount of garbage produced increases exponentially.

The consequences are predictable. Millions of Americans, on the left and the right, now believe things that are unhinged and detached from reality. Because propaganda works. And because the answer to effective propaganda is not "good information" (as the experience of Germany in the 1920s should have taught). There is no shortage of good journalism. The problem is that facts and rational analysis are being drowned in a sea of garbage and propaganda and genuinely fake news.

Our inherited free speech values tell us we must simply live with that. All the conventional norms—people must be treated as autonomous beings to make their own decisions, the answer to false speech is more speech, etc., etc.—tell us we cannot do anything about it. Yet those norms all developed in a world where we could say things like that and not worry too much. They developed in a world where, as a practical matter, our crazed conspiracy theorist and our clever propagandist could only reach a limited audience, and for reasons we didn't really think about and took for granted. The limited distribution opportunities for propaganda before the Internet were like the limited speed of transportation on horses before the car.

> *"The limited distribution opportunities for propaganda before the Internet were like the limited speed of transportation on horses before the car."*

But that's all changed: the costs of taking so much for granted have gone up, way up. Unless checked, they are very likely to spell the end of our constitutional system and of liberal democracy, perhaps not imminently, but certainly over time (and not a great deal of time at that). You cannot run a democratic system unless you have a well-informed public or a public prepared to defer to well-informed elites. Yet we are now rapidly veering toward neither.

One solution would be for the major platforms (Facebook, Google, Twitter, etc.) to pick up the curatorial functions of their predecessors and screen out the awful stuff, making the same kinds of curatorial and editorial choices made by responsible media in the days before the Internet. That's difficult, but not impossible. They already curate in all sorts of ways, and in other countries they block things forbidden by local law. This is no infringement of the First Amendment, because they are private companies. They could self-regulate, in other words, much as the traditional mainstream media did, not to mention the movie and alcohol industries. But they won't, at least not yet. Partly, that's because this undercuts their business interests, but it is also very much driven by conceptions of free speech. People I have spoken with at Google, Facebook, and Apple insisted that I was asking them to be censors, which (they said) violated the First Amendment. (After I noted that the First Amendment didn't apply to them, they shifted to a general free speech norm but still stuck to the same claim.)

Yet this is not asking them to do anything more or different than traditional mainstream media did. Here is another perspective: the major social platforms are, in effect, 21st century newsstands. And like any newsstand owner, they make choices about what to sell and what not to sell. True, traditional newsstand sellers faced technological limits (in the form of physical space limitations) on how many things they could make available. But is capacity the only reason to limit? Didn't moral newsstand owners routinely choose not to sell all sorts of things, from pornography to Communist or KKK propaganda?

Keep in mind that the choice *not* to limit is *still* a choice. As the "new" newsstand, the platforms cannot escape that their decisions about what to allow through their pipelines define what the public sees and gets—meaning they must accept responsibility for the consequences.

So the question we come back to is this: should their conception of "free speech" change because technology enables them to do something that affects the speech market and that was unimaginable in the world where that norm developed?

What about government's role? Should our conception of the First Amendment, of what government can do, change? Democracy has always presupposed a degree of paternalism. The whole idea of representation reflects recognition that popular impulses require a degree of mediation. We rejected direct democracy because experience taught that it leads directly to social unrest and tyranny. True, we articulated a speech norm that looks like direct or pure democracy, but only because (as explained above) in practice it really wasn't. Yet if direct democracy didn't and couldn't work when face-to-face, why on earth would anyone think it more likely to work when enabled on a vastly larger scale by technology? It's still a recipe for social unrest and tyranny, which is precisely what we are seeing.

"… The choice not to limit is still a choice. As the "new" newsstand, the platforms cannot escape that their decisions about what to allow through their pipelines define what the public sees and gets – meaning they must accept responsibility for the consequences."

That being so, don't we have a responsibility to rethink our approach to free speech and government? Should we at least consider enabling government to regulate the platforms in ways we would not have allowed it to regulate newspapers or TV stations, because none of these entities had anywhere near the same power to cause harm? Should we rethink antitrust law? Or the Communications Decency Act?

The alternative to no regulation needn't be that government can therefore do anything. Yes, there is a risk of sliding down a slippery slope. And in the old world that risk was not worth taking. But, today, there may be even greater risk from *not* taking the chance. We already are on a slippery slope—the one created by our extreme libertarian approach to free speech, which is rapidly undermining the foundations of our liberal democracy. Perhaps we should take a chance on the opposite slope and ask whether there are modest ways to regulate speech that can stave off the worst consequences of free speech in the age of the Internet without turning us into a totalitarian state. Most European countries allow limited forms of speech regulation, and they are not appreciably less free than us. At the very least, I think the question needs to be on the table.

"Perhaps we should take a chance on the opposite slope and ask whether there are modest ways to regulate speech that can stave off the worst consequences of free speech in the age of the Internet without turning us into a totalitarian state."

Thread of my recent thoughts about making the Internet-and-democracy conversation more productive.

/1
- I've been thinking about this criticism, which I hear a lot re platforms, democracy, and the election. So, not picking on Ryan here.

/2
- The point of @alexstamos's great thread (as I see it) is to work towards solutions.

/3
- We can't do that well unless we understand the real constraints on possible solutions, including possible unintended consequences.

/4
- We need clarity re which constraints can yield (laws, business models) & which can't (Constitutional limits; limits of technology)

/5
- And we need clarity re unintended consequences of proposed solutions – especially when consequences that hurt democracy.

/6
- I took lots of Alex's points to be about those unintended consequences.

/7
- Saying "it's a crisis" only helps if that shapes what we do. Does it mean "so we should compromise value x that we'd otherwise preserve"?

/8
- If cumulative band-aid fixes like the Honest Ads law aren't enough, next Q is what other value – x – we're willing to compromise.

/9
- Many "democracy-saving" proposals I see work by accepting greater OSP speech control, which hurts marginalized users most.

/10
- Some examples re over-removal disproportionately hurting vulnerable users: washingtonpost.com/amphtml/business/economy…

/11 • Or proposals forfeit key features of modern OSPs (like saying OSPs must be speech police if they use any algorithmic sorting for UGC).

/12 • If "active" OSPs are liable for all UGC, then OSPs must either act like 1993 web hosts or be total speech arbiters. Do we want that?

/13 • Or proposals would entrench incumbent OSPs by requiring filtering technology or hordes of monitors that only they can afford.

/14 • If we can save democracy by hurting just OSP profit, fab. Reallocating $ from tech to save democracy is A-OK by me. Any real ideas there?

/15 • But – spending $ on filters and employees monitoring user speech, in hopes of perfect content regulation by private platforms? Creepy.

/16 • Even if you add better transparency & appeal processes for content takedowns. I like that, but is our goal a privatized justice system.

/17 • I suspect US S Ct case law bars many solutions. It's important to figure out the arguments on that.

/18 • This all leaves me very discouraged about improvements to our Internet and democracy situation.

/19 • Most fixes seem relatively easy but not high impact (tweaks to online campaign ads law, FB labeling 'fake news') or nearly impossible.

/20 • But a lot of smart people think there are things tech (and media, and govt, and NGOs) can and should be doing.

/21 • So let's get clear about facts on the ground and serious parameters like in @alexstamos's thread and get to work.

/22 • I'm done here. Thank you, @united, for keeping the wifi intermittently working long enough for me to get that off my chest. /22 and out

Building an Informed Community

By Justine Isola

Collaborating with Others to Find Industry Solutions

A recent Pew Research Center study found that online news consumers in the U.S. were just as likely to discover news content from direct news websites (36 percent) as social media (35 percent). In other parts of the world, we're seeing similar trends. The Reuters Institute for the Study of Journalism based in the UK. found that 54 percent of online users across 36 countries use social media as a source of news on a regular basis. We don't take these numbers lightly. We know that we have a responsibility to curb the spread of inaccurate information, but we are only part of the solution. All of us - from tech companies and media companies to newsrooms and classrooms - must work together to find industry solutions to strengthen the online news ecosystem.

"We know that we have a responsibility to curb the spread of inaccurate information, but we are only part of the solution. All of us – from tech companies and media companies to newsrooms and classrooms – must work together to find industry solutions to strengthen the online news ecosystem."

In January 2017, for example, we announced The Facebook Journalism Project (FJP), an initiative that seeks to establish stronger ties between Facebook and the news industry. Specifically, FJP is focused on developing news products, providing training and tools for journalists, and working with publishers and educators on how we can equip people with the knowledge they need to be informed readers in the digital age. Since FJP launched, we have met with 2,600 publishers around the globe to create a dialogue around how they use our products and how we could make improvements to better support publishers' needs. We're also making efforts to better explain how our products, like News Feed and Instant Articles, work so that publishers understand how to get more value from them.

Increasing Requirements for and Strengthening Enforcement of Authenticity

People use Facebook to connect with real people, which is why we're so focused on authentic connections and activity on our service. We've built a combination of automated and manual systems to block accounts used for fraudulent purposes such as generating fake clicks or followers, and we are constantly improving these systems to help us better identify suspicious

behavior.

Specifically, we're investing heavily in new technology and hiring thousands more people to tackle the problem of inauthenticity on the platform. Fake accounts are often associated with false news, so this is an area that will have a huge impact on curbing the spread of inaccurate information.

We are also increasing requirements for authenticity when it comes to ads on the platform. Political advertisers will have to confirm the business or organization they represent before they can buy ads. We won't catch everyone immediately, but we can make it harder to try to interfere.

Disrupting Economic Incentives

When it comes to fighting false news, one of the most effective approaches is removing the economic incentives for those who traffic inaccurate information. We've found that a lot of false news is financially motivated. Spammers make money by masquerading as legitimate news publishers, and posting hoaxes that get people to visit to their sites, which are often filled with ads. This results in a disappointing experience for members of our community, who have told us that they expect to see substantive content upon clicking on a post and not be misled.

In order to disrupt these economic incentives, we have taken a number of steps, including:

- Applying machine learning to assist our response teams in detecting fraud and enforcing our policies against inauthentic spam accounts;
- Updating our detection of fake accounts on Facebook, which makes spamming at scale much harder;
- Launching an update so that people see fewer posts and ads in News Feed that link to low-quality web page experiences;
- Addressing a technique known as "cloaking" so that what people see after clicking an ad or post matches their expectations; and
- Blocking ads from pages that repeatedly share false news.

Building New Products

We believe it's important to amplify the good effects of social media and mitigate the bad - to continue increasing diversity, of ideas, information and view points, while strengthening our common understanding. To this end, we are building, testing, and iterating on new products to limit the spread of false news and help people find a more diverse range of topics, news stories, and view points on Facebook.

"We believe it's important to amplify the good effects of social media and mitigate the bad – to continue increasing diversity, of ideas, information and view points, while strengthening our common understanding."

Among the products we've launched is our third-party fact checking tool. We believe giving people more context can help them decide what to trust and what to share. The program we have developed uses reports from our community, along with other signals, to send stories to third-party fact checking organizations. If the fact checking organizations identify a story as fake, we will suggest related articles in News Feed to show people different points of view, including information from fact checkers. Stories that have been disputed may also appear lower in News Feed. Our own data analytics show that a false rating from one of our fact checking partners reduces future impressions on Facebook by 80 percent.

We continue to explore ways to give people more context so that they can make informed decisions about what to read, share and trust. In October 2017, we announced the launch of Article Context to make it easier to learn more about articles that appear in your News Feed. These articles will now include a feature that allows you to access more information at the tap of a button. The additional contextual information is pulled from across Facebook and other sources, such as information from the publisher's Wikipedia entry, trending articles or related articles about the topic, and information about how the article is being shared by people on Facebook. In some cases, if that information is unavailable, we will let people know since that can also be helpful context.

Our third-party fact checking tool and Article Context are just two of the products that we've developed based on feedback from our community and the publishers who are a part of FJP. Our commitment is to continue improving our tools to give you the power to share your experience.

Continuing to Improve

This is an important time in the development of our global community, and it's a time when many of us around the world are reflecting on how we can have the most positive impact. Earlier this year, Facebook announced a new mission: Give people the power to build community and bring the world closer together.
The persistence and spread of inaccurate information runs counter to our mission. Bringing the world closer together depends, in large part, on building an informed community. We have made significant progress in this arena, but we know we have more work to do.

We are committed to improving — not just in the partnerships formed or the tools developed, but in the way we communicate about our choices and the changes we make.

When Freedom of Expression Conflicts with Democracy

A perspective from a Government on the frontlines by Ieva Kupce Ilves

To the broad introductions of the panelists before me there is not much new to say, but I would like to add my perspective or emphasize some aspects as a long time civil servant in the government of a country bordering Russia.

Let me begin with the role of the government. I believe in this situation, like in any other similar of an analogue life, where society or the groups of society or even just number of individuals feel threatened or concerned, the Government is responsible and needs to look into its citizens' problems. As a part of democratically elected government I see no other way than to respond to the needs or concerns of people. The Internet, modern technologies, social networks are new challenges for everyone to adapt and adjust to. For some society groups it might be harder than others, but the recent events of abusing these technologies for manipulation of peoples' votes seems to be a major threat requiring a response across the board – from the private sector and the government to individuals and civic society groups.

"The recent events of abusing these technologies for manipulation of peoples' votes seems to be a major threat requiring a response across the board – from the private sector and the government to individuals and civic society groups."

Leaving the sensitive political issues aside, here is one slightly different example from my experience. In 2010, an anonymous social network called at that time "ask.fm" was created and by 2013 it had about 65 million users; the users were mostly young teenagers. The portal was blamed for becoming a place for cyber bullying and for triggering a number of suicides. While completely in private hands and with no regulation to interfere, Latvian Government received multiple requests by countries or groups of people to involve.

Secondly, about being on the frontline. It is true that outside challenges to democracy are nothing new to the countries bordering Russia and having different political aspirations than its big neighbor like building a strong democracy, and joining the EU and NATO. We probably have been a testing ground for many of the tools exploited today, just on smaller scale that didn't draw much global attention. On the contrary, often we have been perceived as Russophobes that are

just struggling to get over our past. But because of its early concerns about the Internet becoming a new domain of warfare, Latvia launched the NATO Strategic Communications Centre of Excellence in Riga. While at the very beginning we faced the skepticism from Allies and it was not clear if a number of NATO members would support our endeavors, then within a year after the events in Ukraine, where "the little green men" took control over part of its territory, the need became self-evident. Now the Centre has run successfully already for almost three years and I will refer to some of its work later.

As to reinforce a few points of the previous speakers; first, information warfare has been there at all times. Fake news is not new; people and also some governments always have tried to disseminate false information. But what has changed is the scale and the volume. Social networks are incredible amplifiers. In my own country "living in information bubbles" is nothing new, it existed before the Internet took off. After regaining independence, Latvia inherited a large Russian speaking society that only read newspapers or watched TV in Russian. If you read an article from the Latvian press and compared it to the one from Russian, you sometimes couldn't guess that what was described are the same events. Back in nineties the Baltic States were thoroughly scrutinized for meeting democratic principles and so we (the government) didn't dare to interfere in the media world, we aspired to be true democracies. We let those bubbles to live, though we had information on how most of them were financed from Moscow, how propaganda was generated and distributed. We believed that phenomena as time went on, "the free market" and European values would self-correct this. Unfortunately, I have to say that it did not. In our countries we have much higher standards of living comparing to Russia, everyone benefits from the EU, free travel, education, business etc., yet if you will start a discussion with the same people living in this information bubble about political topics you quickly will discover that it sounds like Putin's Russia.

Secondly, about what to do: I think there should be regulation and that there will be regulations in Europe. There are already precedents. Regulations might not be written quite the right way at the beginning, we will make mistakes and we will have to learn, correct and adjust, but I don't believe the free market, private sector or civic groups will be able to fix the problems by themselves in the interest of the greater public good. Given the speed of our daily lives, the multiple priorities and tasks we all

"If an independent expert outside of Twitter or Facebook, like Ben Nimmo of the Atlantic Council's DFR Lab, can trace hundreds and hundreds of bots, then why can't companies themselves do it?

have, I have a feeling that without some rules or a set framework, it will just slip off the priorities list. Not that we have ready-to-use solutions; we have to put those concerns on our priority list, explore and test solutions and then implement those that work. Yes, there might be good intentions in the private sector, but if it doesn't get on top of priorities they will not be implemented.

For example, though I am not technical expert, I do not understand why we can't eliminate bots and fake accounts. If an independent expert outside the Twitter or Facebook like Ben Nimmo of the Atlantic Council's DFR Lab, can trace hundreds and hundreds of bots, then why cannot companies themselves do it? They, after all have a far bigger picture of the problem as well as better information on the bots? And why can't those bots just be stopped? Here is a tiny example from the NATO STRATCOM COE research, which they made at a time, when NATO reinforced its military presence in the Baltic States and Poland. The Centre monitored social networks and learned that 84% discussion in the Russian language about this topic was bot-generated. Less but still almost half – 46% in the English-language domain were bots. So are we arguing about and defending the freedom of speech for bots?

However, regulations are not enough, it might not even be the most important element; I just felt to put an argument in support of it. Governments need to become better in communication with society. It is the responsibility of government to provide information and explain its work to the people (though it also leads to a question of governments' performance and not merely PR). Yes, Governments are the last and the slowest to adjust to any new changes and we are handicapped in today's situation because of the speed and characteristics of online world. If you look at the most of tweets or posts that go viral, they are all about emotions. It is not about the facts, but the emotions that the posts succeed with. So imagine now the government's regular press release: how many re-tweets will it get? How do we convey the facts and information of the sometimes rather complicated and boring work of the public sector to people in this new environment: to be short and emotionally attractive? Still, that is something we, Western democracies all have to put an effort in.

"If you look at most of the tweets or posts that go viral, they are all about emotions. It is not about the facts, but the emotions . . . How do we convey the facts and information of the sometimes rather complicated and boring work of the public sector to people in this new environment: to be short and emotionally attractive? . . . This is something we, Western democracies all have to put an effort in."

Reflections on When Information Becomes the Weapon

By Mike Brown

The problem we face today is very big and the technology of the internet makes is quantitatively and qualitatively different from what we've seen before: internet technology means that the messages have a wider reach, tailored content and obfuscate both their source and veracity. As a result, this is a supreme propaganda tool being used against our own citizens by our adversaries. What we've seen recently is beyond the scope of anything we've seen in our history and while we're focused more on what Russia did in the 2016 election, China has an equal capability to influence us through an army of government employees whose job it is to develop and distribute propaganda in a systematic and continuous way.

"In one year alone, 450 million social media posts—roughly one in six—were fabricated in China. This is part of one of the most impactful global information operations campaigns since the end of the Cold War but it has largely gone unnoticed. China has been expanding its information operations campaign globally as well, portraying itself as the protector of internet stability. This narrative, promoted against the backdrop of U.S. investigations into Russian hacking and a broader U.S. retrenchment from global leadership, diverts attention from the realities of China's great firewall, decades of digital intellectual property theft, and domestic surveillance. China's leadership has mastered the art of domestic diversion and is now doing the same thing globally to promote its own model of cyber sovereignty. From Davos to the United Nations, China is putting a stake in the ground to shape the future of the global internet."[1]

It has to be the U.S. government responding because there is no single company that has the resources to fight back. The scope of the problem is so broad (IP is stolen which affects private companies, but national security information is also stolen). Until there are some meaningful consequences to the tremendous level of malicious cyber activity, it will continue to increase and create ever more damage to our economy, our information and our institutions.

"Until there are some meaningful consequences to the tremendous level of malicious cyber activity, it will continue to increase and create ever more damage to our economy, our information and our institutions."

Today it is Illegal for a company to hack back or counter-attack these (even if it were allowed, this would create anarchy). It has to be the U.S. Government responding to state actors. The government can also play a role in helping the private sector defend/protect itself by sharing more timely information with the private sector about known threats. Today this is too often a

[1] Andrea Little Limbago, "China's Global Charm Offensive," *Endgame.com*, August 28, 2017

one-way request to share information with the government. There also needs to be a unified answer by sharing best practices with the private sector and perhaps improving firewall and detection capabilities within our IP providers and telecommunications networks.

News organizations (which now includes social media) have a responsibility to vet sources which appear widely or at a minimum be transparent that sources cannot be confirmed or provide information as to the source if they are foreign governments or foreign news agencies. We need to acknowledge that Chinese and Russian news agencies are instruments of state power. Personally, I think it's irresponsible not to block these propaganda instruments when we know China or Russia is responsible since our freedoms and values are viewed as existential threats to their regimes (as detailed in *Document 9: A ChinaFile Translation, November 8, 2013).* We cannot treat these state instruments of power the same as independent news agencies which do their best to report news.

"Today it is illegal for a company to hack back or counter attack . . . it has to be the U.S. Government responding to state actors. The government can also play a role in helping the private sector defend itself by sharing more timely information about known threats."

We are in an ideological war. Russia and China are waging this now. We must respond because it is naïve and dangerous not to respond. China has recently publicly declared its strategy with respect to becoming a super power in cyberspace and this strategy relies on managing internet content and distributing it worldwide. This document details that "the [Communist] Party's ideas always become the strongest voice in cyberspace."[2]

Finally, we need to improve our capabilities to do forensic work on attacks even though this is already quite good within the FBI and NSA. We need to get more comfortable naming who is responsible for attacks and imposing a cost to foreign governments behind these attacks. State employees moonlighting should be treated as state-sponsored attacks since we know that Russia at least tacitly approves of the talent within their equivalent of cyber command moonlighting for personal gain and creating damage by hacking Western companies.

[2] Elsa Kania, Samm Sacks, Paul Triolo and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated", September 25, 2017. Retrieved at www.newamerica.org.

Transcript of Timothy Garton Ash's Ten Points to Frame Challenges to the Quality of Discourse in the Digital Age

October 6, 2017, Encina Hall, Stanford University, Stanford CA

Well, first of all, congratulations on what sounds like a terrific initiative - another great initiative in this area at Stanford. I mean, as we all know, free speech is indispensable to democracy. Josiah Ober, a great scholar of this university, has demonstrated that it was present at the creation of ancient Athenian democracy. And by the way by free speech we mean at least three things: Freedom of expression, which is in our title, Freedom of Information, which is just as important, and a certain quality of democratic discourse or debate. There's something about the quality of the speech. Now, so, as both Mike and Eileen said, it's a case of old principles in dramatically new circumstances. Now I think the first thing to say is that the Internet as a whole has been a fantastic gain for the kind of freedom of expression and information we need for democracy. That needs to be put out there. We have unprecedented access to information, to evidence, to ideas from across the world. I love my twitter feed. I think Pericles would have loved his Twitter feed. But, as always happens with technology, if there's a big upside, there's a big downside. That's true of all technology through history. It was true of printing, obviously, and thinking about the downsides, which we're now focusing on… Larry… since Larry set me up for this like that Gilbert and Sullivan character, I have a little list. And I'm going to go through it at Gilbert and Sullivan operetta speed, but I think it's useful just to lay out a

few headings. Okay, so I've got ten, and it's not complete:

Number one – sheer quantity. That's the flipside of the positive. [There is] a lot of criticism of Facebook, some of it justified. How do you monitor billions of items of content coming up in 200 languages every day? That's number one.

Number two – if we believe that the state does have a legitimate role in regulation on, for example, extreme pedophile child pornography, or on terrorism, then the frontier hopping quality of the Internet – information, ideas, images sweeping across frontiers – makes that legitimate function of the state more difficult.

Number three – democratic discourse requires a quality that I try and capture in the phrase "robust civility". So, it's not just civility. It's not just having tea with the Queen. Its robust civility. There's nothing you can't talk about, but you talk about it in a civil way. It's what we try to do in Universities. Now, the way the Internet has developed produces a big challenge to this. It's partly because it's not face to face. It's partly because much of it is unedited. it's partly because it's very quick, so people tweet and then think rather than the other way around. It's also because of anonymity. There's very good work demonstrating that anonymity contributes greatly to incivility. Actually, if you write a guardian column you know that anyway, you just see the comments. Not just incivility, [but] hate speech, harassment, cyber bullying, death threats. I've never forgotten a comment made to me by the Canadian liberal feminist Muslim thinker Irshad Manji, who gets many, many death threats, and she said, "Tim the person who is usually threatening me with death is called anonymous". But at the same time anonymity is essential for people living in dictatorships or oppressive communities, so we have a problem there.

Okay, number four follows from that – impersonation, which is slightly distinct. Impersonation. You think you are being addressed by a fellow American voter [but] in fact you're being addressed by a Russian bot. We used to say "on the internet no one knows you're a dog," and now we say, "on the internet no one knows you're a bot." And, actually, the development of AI, the rapid development of AI, contributes enormously to this. I saw paper the other day which envisioned a wonderful dystopian future in which the internet would mainly consist of billions of bots trying to persuade or sell things to other bots, each thinking that the other was a human being, which I think is a rather wonderful, hilarious dystopia.

This leads on more seriously to number five – disinformation and misinformation, the subject of the next panel. Disinformation, by which I mean false information maliciously disseminated for political reasons. By misinformation, I mean false information maliciously disseminated for other reasons (for example, money - Macedonian meme farms). Now, this is a big problem. It leads on to an even bigger one which is… there is good work that shows that misinformation - false information- is as likely to go viral as reliable information. That's pretty well established.

So, and this is point number six, you have a balance between what I call virality and veracity. If you believe that veracity is a quality you need in media endemic for well-informed citizenry,

then if your algorithms privilege virality, you have a problem. So, there's a question to the Facebook newsfeed algorithm.

Number seven, mentioned already: homophily, echo chambers, filter bubbles. What I would just say quickly on this, to emphasize again what Mike and Eileen said, we need much more research on this. It is not well-established where and what exactly is the echo chamber effect, and for that we need the data from Facebook because otherwise we can't do the research.

Number eight follows from that – the impact on established media. The fact is the business model of most newspapers in the Western world has been blown out of the water. They are all struggling for survival. This means they do less serious investigative reporting, much less foreign reporting. They sensationalize, they shout in order to try and get the click stream. That's a serious problem for the quality of our democratic discourse.

It goes to point number nine in the Gilbert and Sullivan list which is a very important one, only now becoming salient – the tendency to monopoly. There is a very clear tendency to monopoly because of networks, network effects and other reasons on the internet. Intrinsically – Google, Facebook, Twitter, Amazon, Apple, what the French call “le GAFTA” what I call the private superpowers – intrinsically, that is a potential danger for democracy. Any study of quality of democracy will have a criterion which is media pluralism, so if you don't have good media pluralism…

Number 10, not quite so obvious, but I think important, is the erosion (online) of privacy and the potential for mass surveillance. I say

the potential, not necessarily the actuality, because even potential Big Brothers are a danger for democracy.

Okay, so that's my little list, Larry. It's not comprehensive. One might be tempted to say, looking at that, “bloody hell what a what a bloody, to not use a stronger word, tsunami of bad stuff coming at democracy from the Internet. Isn't it going to engulf us?” I would warn against mood swings from the extreme of cyber utopian optimism of the 1990s to the kind of cyber fatalism of today. Actually, what we have to do – we who believe in both free speech and

democracy – is to keep working to maximize the positive, the upside, which is still very big, and minimize the downside. That, in the most general terms, is what we have to do. Last point, Larry who is “we” in that sentence? We’ll come back to this, I’m sure, in discussion. In my book, I talk about the big dogs, the big cats, and the mice. The big dogs are the states and their governments. The big cats are Facebook, Google, Twitter, Amazon, Apple, what the French call “le GAFTA.” I call them private super powers. And the mice are us, the citizens and netizens, collected in smaller entities in think tanks, in NGOs, in universities, in civil society. On each of these points that I've mentioned and any others that will come up, the question I think we have to ask is, “what do we want each of these three sets of actors – governments, companies, and civil society – to do in what interaction with each other?” I mean, I think that's the structure of the question on each point. Now Larry I have, as you know, some views on that, but I think in the name of robust civility I should let someone else speak.

Transcript of Keynote with Secretary Hillary Clinton

October 6, 2017, Cemex Auditorium, Stanford University, Stanford CA

Remarks and Q & A

[BEGIN]

Secretary Hillary Rodham Clinton: Thank you very much. Thank you all. It's great to be back here at Stanford, and I want to thank the President and the Provost for welcoming me.

The idea of this event, the timely launch of the Global and Digital Policy Incubator could not be at a better time or place. I know there have already been important panels that have discussed important issues, and I look forward to sitting down with Eileen Donahoe. I also want to recognize Secretary of the State, Secretary of Labor, Secretary of the Treasury, George Schultz. It's wonderful that he's here and it's always a treat for me to see him.

Now this is a timely conversation because our country, and all democracies, face serious and urgent challenges from the nexus of technology, propaganda, terrorism, espionage, and cyber warfare. In the 19th century, nations fought two kinds of wars – on land and on sea. In the 20th century, that expanded to the sky. In the 21st century, wars will increasingly be fought in cyberspace.

As Americans, we need to approach this new threat with focus and resolve. Our security, physical or otherwise, cannot be taken for granted. At the same time, when it comes to technology, we have as much cause for optimism and excitement as we do for caution and concern. So the question is how we strike the right balance. I've seen, as you all have, the ability of technology to improve our democracy and empower people.

As Secretary of State, I made it a priority of U.S. foreign policy, encouraging the development of deployment of new tools to shine a new light on human rights abuses and help citizens hold their leaders accountable. We also worked to help keep dissonance safe online and to train activists around the world, working with designers to create new apps and devices, including a panic button that a protestor could press on their phone that would send a signal to friends that he or she was being arrested while simultaneously erasing all of their personal contacts. I gave a speech in January 2010 about internet freedom, laying out the stakes that America and the free world have in its preservation. It was Eileen Donahoe who helped pass the first U.N. resolution on internet freedom as her time as U.S. ambassador to the Human Rights Council.

Of course, here in the U.S., technology has opened up our political process. Howard Dean got the ball rolling with his groundbreaking campaign back in 2004, and then Barack Obama took it to the next level in 2008 and 2012. My campaign continued this process of using technology to make it as easy as possible for Americans to participate in the democratic process. When people were being turned away at the polls on the last day of early voting in North Carolina because they didn't have the proper ID, they tweeted at us. Election protection volunteers in Brooklyn were able to help them in real time so they could cast their ballots.

Thanks to advances in technology, it's simpler than ever before to learn about local elections – everything from the details of candidates' platforms to the locations of polling places. It's now possible to make voting more accessible for people with disabilities or the elderly, enlarging the font size on ballots, or even voting by voice command. And it's easier than ever to volunteer, donate, and make your voice heard.

This is all good and healthy for our democracy. But, as we all now know, the 2016 campaign also revealed a darker side of the intersection of technology and democracy, with a brazen assault by a foreign adversary determined to mislead our people, enflame our divisions, and throw an election to its preferred candidate. This is an ongoing threat – a clear and present danger to our democracy. That same adversary is counting on the fact that America and its leader will be too proud, too weak, or too shortsighted to face this threat head-on. For generations, Americans have come together to defend human rights, defy totalitarianism, and stand up for democracy around the world. I believe we have what it takes to understand what happened in the 2016 election, act decisively to make sure it never happens again, and confront this threat to western democracy.

Let's start with what happened, which does happen to be the title of my new book. If you want to dive into these issues more deeply, there's a lot more on all of this in there. Now, there were many factors that influenced the outcome of the election. It was, in fact, a perfect storm. But today I will focus on the information warfare waged against us from the highest levels of the Kremlin. A flood of new revelations has come to light in the last 24 hours alone, and I believe there will be more, so stay tuned. Here's what we know right now: To drive a wedge between Democrats just as we were coming together after the primary, Russians hackers stole and selectively published files from the Democratic National Committee. It was a virtual Watergate break-in. Later, to blunt our momentum and distract from the Access Hollywood scandal, they released emails stolen from my campaign chair John Podesta. Russian operatives forged documents to fool and manipulate the FBI. They probed voting systems in at least twenty-one states, possibly as many as thirty-nine. Stop and think about that for a minute: the Russians hacked our election system. We're only beginning to learn the extent of what they accomplished. And it doesn't stop there.

To confuse and mislead voters, the Russians used state-funded propaganda networks like RT (formerly Russia Today) and Sputnik to spread disinformation. As the U.S. Intelligence Community has reported, Russia also used trolls, bots, fraudulent accounts, agents posing as Americans, and fake groups to game social media networks and search engines. They "flooded the zone" with attack ads and negative stories intended to whip up support for Donald Trump, suppress support for me, and create fissures in our society. Thousands of trolls carefully disguised themselves as Americans – Muslims, Black Lives Matter activists, second amendment advocates, and more. Some even staged fake demonstrations in Florida and Texas. And the Russians weren't just shouting into the void, hoping someone would notice. The propaganda was aimed directly at undecided voters and "soft" Clinton supporters who might be persuaded to back a third-party candidate or not vote at all. In particular, they were trying to demoralize, disillusion, and demobilize the traditional Democratic base, and get them to stay home on Election Day. In fact, we learned just this week that some of the Facebook ads specifically targeted Michigan and Wisconsin – two of the states that decided the election by razor-thin margins, which suggests that the Russian strategy was even more sophisticated than we knew.

This was information warfare on a massive scale. Mike Morell, the former acting director of the CIA, has called it "the political equivalent of 9/11." Former Director of National Intelligence Jim Clapper described it as "a threat to the very foundation of our democratic political system."

Special Counsel Robert Mueller and congressional investigators are working to determine whether there was any collusion or coordination between the Trump campaign and the Russians. But we already know that Trump publicly cheered on the Russian operation and took maximum advantage of it – helping hand Putin his victory.

What's more, the entire operation was especially successful because our country's natural defenses had been worn down for years by powerful right-wing interests – from Fox News and Breitbart to bogus, climate-denying think tanks funded by the Koch Brothers -- that worked to make it harder for Americans to distinguish between fact and fiction. Did all of this have an effect? Of course it did. To suggest that a campaign of this size and scope had no impact at all is to write off the same kind of persuasion advertising that both major political parties have spent billions of dollars on in recent decades. That argument just doesn't hold up. As Mike McFaul points out, even if Russian interference made only a marginal difference, this election was won at the margins – by 78,000 votes in three states: Pennsylvania, Wisconsin, and Michigan. Wisconsin was decided by fewer than 23,000 votes. Michigan, less than half that. The Russians set out to intervene in our election by taking aim at the heart of our country's strength, our democratic institutions. Both common sense and evidence indicate that they were successful. And make no mistake: this isn't just about what happened in 2016; it's about what's happening right now, as we speak.

The Russians are still playing on anything and everything they can to turn Americans against each other – whether it's the violence in Charlottesville, the controversy over NFL players "taking a knee," and now, the massacre in Las Vegas. Thousands of social media accounts with suspected ties to Russia are posting, in some cases on both sides of all of these issues, to fan the flames of division and weaken us as a country. In addition to hacking and influencing our elections, the Russians are hacking our discourse and our unity. This helps reveal Putin's true agenda. Yes, as the intelligence community says, he had a personal grudge against me. But this goes far beyond that. Putin's goal is to weaken the Atlantic Alliance, reduce America's influence in Europe, and threaten the foundation of western democracy itself.

In Germany, members of Parliament have been hacked by Russians. In France, Emmanuel Macron's campaign was hit by a massive cyber attack just before their presidential election. Russian agents pushed incendiary social media posts last weekend during the Catalonian independence referendum, which is rocking Spain. Their weapons of choice may not be tanks or missiles, but let's not mince words:

This is a new kind of cold war. And it's just getting started. What can we do about it? I believe there are five steps we must take.

First, we need to get serious about cyber security. Government and the private sector need to work together to improve our defenses against future cyber attacks, including by making necessary investments to protect our networks and national infrastructure. Corporate America needs to see this as an urgent imperative, because government can't do it alone. At the same time, our military and intelligence agencies should accelerate the development of our own offensive cyber and information warfare capabilities, so we are prepared to respond to aggression in kind, if need be.

Right now, we do not have an effective deterrent to prevent cyber warfare the way we do conventional and nuclear conflicts. It's time for the U.S. to declare a new doctrine stating that a cyber attack on our vital national infrastructure will be treated as an act of war and met with a proportional response. I agree with Toomas Hendrik Ilves [ILLvz], the former president of Estonia currently at the Hoover Institution here at Stanford. In response to the news that Russia targeted NATO soldiers' smartphones, he proposed a global "cyber NATO," to present a united front in the face of these threats. As he rightly points out, "the liberal democratic West has been subjected to enough wake-up calls." Getting serious about cyber security also means that the federal government can't just gather intelligence and keep it under lock and key; they need to share it quickly with local election officials who can act on it. Let's make sure our intelligence community has the tools to detect an operation and warn us before it can influence our democratic process, not after it happens.

The Graham-Klobuchar Amendment in the Senate, and the Meadows-Langevin [LAN-juh-vin] Amendment in the House would do just that, and passing them would be an important step toward safeguarding future elections. In the meantime, I'm encouraged by emerging initiatives like the Alliance for Securing Democracy, which is working to develop tools and strategies to counter this unprecedented attack on the United States and our allies, and track the full toolkit Russia is using to undermine democracies. If you haven't seen it yet, check out the dashboard they've created to track Russian active measures at dashboard-dot-securing-democracy-dot-org.

Second, we need to get tough with Putin. It's been said that he subscribes to Vladimir Lenin's old adage: "Probe with bayonets. If you encounter mush, proceed; if you encounter steel, withdraw." When Putin looks to America, he should see steel, not mush. I was encouraged that earlier this year, over the President's objections, Congress passed bipartisan legislation to ratchet up sanctions against Russia. But months have gone by with little or no action or enforcement from the administration. Senators John McCain and Ben Cardin have rightly called on the President to enforce the law, and expressed concern that the sanctions may even have already been violated. As recently as this week, a key deadline in implementing the sanctions came and went. This is shameful. The President swore an oath to faithfully execute the law and defend our Constitution. He should do his job. And the rest of us have to keep up the pressure. No foreign power in modern history has attacked us with so few consequences, and that puts us all at risk.

I'm not holding my breath for this White House to do any of this, but it bears saying: The United States should also strengthen NATO's cyber defenses; help our allies reduce their dependence on Russian energy supplies, which are a key source of leverage for Putin; and arm the Ukranian government so it can resist Moscow's aggression. I'll leave it to Special Counsel Mueller to decide whether or not there was collusion. But we don't need a lengthy investigation to tell us that Trump is ignoring the intelligence community about an urgent threat, refusing to stand up to an adversary that has already attacked us, and abdicating his responsibility to preserve, protect, and defend our national security. We have all the facts we need on that one.

Third, we need to close legal loopholes in our election process. More than ever before, elections are won online. But too often, we're using analog laws for a digital world. All digital political and issue advertising should have a disclaimer and be reported to the Federal Election Commission, just like television ads. If a person or group is influencing the information people consume before an election, they should have to be transparent about it. And foreign entities should be banned from issue advertising or political advertising in any medium. They aren't allowed to contribute to American candidates, and they shouldn't be able to support them with ads either. Fourth, we need to get to the bottom of what really happened in 2016 and develop real strategies to halt this activity now and in the future.

The Special Counsel investigation should be complimented by an independent commission with subpoena power, like the one that investigated 9/11. It should provide a full public accounting of the attack against our country and make recommendations to improve security going forward. Americans and the world need to know the truth about what the Russians did, and that includes a comprehensive, honest accounting from companies like Facebook, Twitter, and Google.

A few days ago, Mark Zuckerberg expressed regret for the way Facebook "was used to divide people rather than bring us together." But remorse alone won't heal our divides or protect our democracy. Facebook itself has acknowledged that it sold $100,000 in ads to fake Russian accounts during the election. Those ads were seen by at least 10 million people, in crucial states. New research out just yesterday from Jonathan Albright at Columbia's Tow Center for Digital Journalism found that content posted by Russian trolls and bots had been shared upwards of 340 million times. And even that could be just the tip of the propaganda iceberg.

So it's time for Facebook to demonstrate real transparency and accountability. They are the largest news platform in the world. With that awesome power comes great responsibility, which they must accept. It was also disappointing to hear Senator Mark Warner's original report that Twitter's closed-door briefing for congressional investigators was, quote, "inadequate on every level." It's time for Twitter to stop dragging its heels, and face up to the reality that its platform was – and is – being used as a tool of cyber warfare and propaganda.

Silicon Valley has already shown that they can be part of the solution, not the problem, when it comes to ridding the Internet of child pornography. We're starting to see progress in confronting online terrorist recruitment.

Now, companies like Facebook, Twitter, and Google need to show that same commitment in addressing fake news and propaganda. They are more than capable of figuring out how to continue to innovate while expanding transparency and complying with disclosure rules, just like everybody else. Fifth, we must fight back against the assault on truth and reason and rebuild trust in our institutions. I agree with Tim Cook of Apple that we need a "massive campaign" against fake news. The mainstream and online media have crucial roles to play in debunking the lies and holding liars accountable.

And ultimately, it's up to each of us to stay informed, and make good decisions with rigorous reasoning and fact-based deliberation. Let's start early, by teaching our youngest learners to be critical thinkers who value facts and evidence. We all have the ability to break out of our echo chambers and engage with people who don't agree with us politically. We can keep an open mind and be willing to change our minds from time to time. Even if our outreach is rebuffed, it's worth it to keep trying.

We know Putin and the Russians are doing everything they can to divide us – why would we help them along?

We're all going to share our American future together. It's better to do so with open hearts and outstretched hands than closed minds and clenched fists.

I know there are some people who don't want to hear about these issues, especially from me. But I am going to keep sounding the alarm. We cannot dismiss this as a hoax or of limited impact; we have to confront it head-on. This is a perilous time at home and abroad. Like a lot of people, I'm deeply worried. But I am also confident that with American innovation and patriotism, and the insight and leadership of the farsighted thinkers in this room and across the country, we can show that extremism and authoritarianism are no match for democracy and free-thinking people.

I'm looking forward to talking more about these issues now, and in the weeks, months, and years to come. So with that, I'd like to start my conversation with Eileen.

[Begin Seated Q and A with Eileen Donahoe and Larry Diamond]

Eileen Donahoe: I must admit, a part of me wishes you were not able to be here.

[Laughter]

Secretary Clinton: Me too.

[Laughter]

Donahoe: And in fact that maybe you were off solving a diplomatic crisis with North Korea, or something like that. But in all seriousness, your story, and how it relates to digital technology and democracy, is not only valuable for historical record but at the end of the day, your story is our story, because it's really about what happened to our country, what happened to the security of our democratic processes and the quality of our civic and political discourse as you've said. And here at Stanford and Silicon Valley we have a very great vantage point as you say, we bear great responsibility with addressing these issues.

So let me very quickly mention especially to the students we are going to try to take some questions from you, and if you could just pass questions on the cards to the end of the aisle let's say in the next 20 minutes, that would be great. So I want to start on a somewhat philosophical level in fact with the (fifth?) point you just raised. And I want to talk about truth.

Our Declaration of Independence opens with the phrase, "we hold these truths to be self evident", and we were founded on this almost meta-physical assertion about truth as the basis of our political union. Access to information has been the lifeblood of our democracy, but as you describe the potent mix of digital misinformation, trolls, bots, microtargeting hate speech, have all eroded our confidence in the veracity of information we get online. On top of the problem of misinformation, which is very real, we now have some politicians calling any news they don't like, fake news. And this erosion in the confidence of truth itself, has been so great that the Oxford Dictionary chose, "post truth" as the word of 2016.

So simple question, what happened to our belief in truth? And beyond technical fixes, which we were trying to discuss today, what can we do to try to restore our cultural commitment to truth and factual analysis, as the basis of our political discourse and policy?

Secretary Clinton: Well that's an easy question to answer

[Laughter]

Secretary Clinton: But it probably is truly one the most profoundly important issues we face.

Let me just tell you from my perspective, in my book I write about the success of the Russian operation in light of—and I have a metaphor I use, the body politic needs to have a good immune system, just like the physical body to ward off attack, and our national immune system has been worn down over the last decade, some of it the fault of the government lets be very clear. Misleading the people about all kinds of important issues, raising divisive concerns for political advantage.

So I think our institutions and the leaders of our institutions going back for decades, bare some of the responsibility for a very partisan environment in which people were accused and the truth was made more elastic than it should have been. I think something in addition and different has been happening and I alluded to it in my remarks.

There has become a industry of fabrication, for the purpose of gaining advantage, commercial advantage, partisan advantage, ideological advantage, and it has battered the immune system of our body politic and it has been accelerated and made all pervasive because of the advances of technology.

You know there is that old saying that a lie can halfway around the world before the truth pulls on its boots. Well now, you know it’s a nanosecond it's just impossible to combat the flood of false information, that is being put forth (served?) the ends of various powerful interests. So I feel like we were somehow we were meek-end over the last years to the point that the way the Russians understood propaganda, because they have long, long history with kompromat and active measures as they're called, they knew that there might well be vulnerability that they

could take advantage of, and I think they were quite clear and unfortunately accurate in believing that.

What do we do?

Well we have to begin with at least once again by pledging our allegiance to fact based deliberation, evidence based policy making, you know it's very discouraging. It's one thing to lie for partisan advantage it's something entirely different when you do it over and over again with every technological tool at your disposal.

So we've just gone through this debate about the affordable care act. It was clear for the people advocating for the changes had no idea what they were talking about, it was just painfully obvious and they couldn't withstand the simplest of interrogation, but they stuck with their talking points. Go out there and say this over and over again. And unfortunately, too often in our media, with broadcast and press—written press—you know reporters don't go to the second or third level because and they get wrapped up in this false sense of fairness, like okay you said this and you turned to the other person and they said that and there is no real pressure for pinning people down about the falsehoods. We see the same things starting with the tax bill argument. So they're coming out and they're saying you know we're really gonna do great things for the middle class. I mean it absolutely defies arithmetic for them to be able to make that claim. Forget words, just look at numbers. And we know once you dig into it they're going to cut a trillion dollars from Medicaid and $450 million dollars from Medicare. That's the fact.

You know people said that the healthcare bill was a tax cut parading as a health care bill. This is a tax cut that is going to destroy health care over the next few years. With the ways that it will decimate public budgets. Now these are real world examples in our own political environment. And we've gotten used to people not being held accountable for any kind of truth.

So if we don't start in our own home, and we don't have better interrogation in the media for people that are making these claims, it's really hard to protect ourselves against the onslaught that is coming from the outside whether it is the Russians or anyone else. So honestly, I think

this may be one of the biggest problems we face as a society and you know higher education has a particular role to play, the press has a particular role to play, people have to be held accountable for their misstatements and their use of climate change denial to further their profit margin or any other reason that they are doing that. And if we don't hold them accountable, we can't expect voters and citizens to understand the back and forth that goes on so we all have an obligation to stand up for the self evident, even if they're not self evident, these evidence based facts and truths.

Donahoe: So I want to turn it back to the national security front, which you've raised. And we've talked about how unsettling it is that the Russians have such sophisticated ability to hack into and manipulate our civic discourse, so much so that they were able to actually change the outcome of our election. For me the peculiarly challenging part of this, for Americans, is having to see information as a weapon.

Our cyber security experts will prepare you for there is some type of cyber to kinetic attacks on infrastructure, some were anticipating attacks on voting machines, maybe not adequately, but at least thinking about it. But most—almost no one was prepared for an attack on our civic discourse, as a means of affecting the outcome of the election. So why do you think we were so unprepared as Americans for that particular threat, and what is different now about fake news in the digital realm from propaganda we have seen for generations.

Secretary Clinton: That's a great question too. I think part of it was the unprecedented nature of it.

So the first time something happens, it is hard to believe. By the time it happened to us that sent fair warning to the Dutch, and the French, and the Germans, so that they were better prepared to defend their own elections, against the ongoing efforts. And the Russians and their allies, created a couple of big mistakes in the French effort in trying to dump a bunch of hacked emails the Friday before the Sunday vote, not realizing in France there is a law that you can't have any news about the election 72 hours before the election.

So what they hoped to see happen couldn't happen, and they also made it possible for macron and his campaign to get prepared by seeding their email accounts with false emails that they could then point to.

So we didn't have that precedent, we didn't have that advantage of being able to say well that happened to the French. We should have probably have understood more of what happened to the Brexit vote because that's a different but equally troubling use of targeted data used to influence voter decisions. But we didn't really draw a connection between that and the Russians and when we started to get news about the Russians hacking into the DNC and Trump calling to the Russians to find my emails and all of the stuff he was doing, it was hard to evaluate how serious that was and what difference that was going to make.

So I don't want to excuse everybody, including myself and my campaign, but we couldn't get the press to take it seriously because it had never happened. And it seemed like some argument we were making to gain political advantage, instead of trying to sound the alarm which was what they thought we were doing. And it just got more and more sophisticated, actually a year ago tomorrow, October 7th, was one of the most important days of the campaign, because three things happened. In the morning Jim Clapper, the Director of National intelligence, and Jane Johnson the Secretary of Homeland Security, made for the first time, really an official public statement that the Russians had hacked information and were trying to affect our elections.

That happened in the morning. A few hours later the Hollywood access tapes dropped, and that pretty much obliterated any sort of attention that anyone was paying to the homeland security leaders were saying. Any within one hour, Wikileaks, which basically has become a wholly own subsidiary of Russian intelligence, dropped the Podesta emails. And it worked like a charm, and why did it work?

Well it worked first because the Hollywood Access tapes just blew up the media for about 48 hours. It was just on a loop constantly, constant. And then it kind of dissipated. Everybody's seen it. They drew their own judgments, and go from there. But dumping 1,000 WikiLeaks pages of Podesta's emails day by day kept that issue alive, and it wasn't just that they would

just publish them, they then had a very sophisticated operation to do what we call “weaponize” them.

And the most egregious example, perhaps some of you have followed it, Podesta had some email about going to a pizza parlor in Washington DC. I mean when you read it it seems super innocuous; doesn’t seem like it means anything other than he likes pizza. And uh, next thing you know, the outlets on the right, some of them you know, Brietbart, InfoWars, took that email and turned it into a fake news story that John Podesta and I are running a child trafficking ring in the basement of this pizza place. I mean when you see that, you think who would believe that, well a lot of people believed that. Unfortunately, more than I wished. More than I could have imagined. And it’s not even just being put out on those sites, it’s being reported on our “T” which then gets picked up on Facebook posts and then gets targeted to people based on whatever sophisticated targeting they are using to the extent that a guy in North Carolina, is just bombarded by it and decides he has to go rescue the children, so he loads up his automatic weapons and barges into the pizza parlor with his AR-15 and shoots up the place. Of course discovering there is no basement, and there are no children.

Luckily no one was injured. But the power of that one example is enough to make me understand how effective the coordinated effort was between the Russian theft, the passage to it, cutting it out, putting it on Wikileaks, dropping it at a strategic time, and weaponizing all of these various emails to make the most outrageous claims, that were meant to suppress voters or change voters mind. So this was not just idly done, this was very carefully planned and carried out, and I think what former President Ilves pointed out in his remarks, this is going to continue and that’s why we need to figure out how to combat it, and we are going to need to educate people so they are never surprised again.

Donahoe: So you touched on earlier the subject of digital insecurity and the need for education about that. You struggled with the challenges of lost privacy, and you also raised the problem with our ethos around doxing.

So when John Podesta’s email was hacked and doxed the mainstream media was just basically gleeful about it, and they dragged out all of the reporting on all that mundane stuff, but they somehow the very, very big story that this doxing by WikiLeaks was an act of political sabotage, with gargantuan national and global security issues.

So why did the mainstream media fail that basic test, and fail even to see the consequences of their own unbenign(?????) participation in that sabotage, and what can we do about that ethos?

Secretary Clinton: I think that has to be part of the investigation, from here (???) in this new project, because I think you've got to get behind the decision they make in the quote "mainstream media" to really understand that. I mean from my outsider, observer status, I think that part of it is that if people think that something looks like its secret it's got to be more authentic.

Ok we all saw Trump admitting to sexual assault and ok fine, let's move on, let's talk about John Podesta's love of pizza, there's got to be something really interesting in there. I honestly think it's just kind of the way our minds work. You know if it's a little bit harder to get than maybe it's got a little bit more authentic meaning. In the book, I talk about how we track google searches. So after those first couple days, Google searches, of Hollywood access were pretty low, everybody saw it, nobody had to search for it.

But google searches about Pizzagate, that just took off, because everybody wanted to know what's really going on, and oh my gosh how can I vote for someone that might be running a child trafficking ring.

So I think that like everybody else, to give them the benefit of the doubt, that the mainstream media didn't really accept or believe what we and others were telling them, including our intelligence leadership and homeland security leadership. And it put them in a position where they said, well we don't really know if this is true we don't have any concrete information, if you remember the FBI would never confirm if there was an ongoing counterintelligence investigation between Trump and the Russians. Don't get me started.

[Laughter]

That was something that was pretty hard to understand. But if you're making decisions in a newsroom, well you know the FBI isn't confirming it, so maybe it isn't true! But oh my gosh these WikiLeaks, here's John Podestas risotto recipe, which got huge google hits! So it's not only the deliberate effort to plant false stories, it's such a great distraction.

Don't let people look at what's really going on, which will have long term consequences for ourselves and the world, keep everybody chasing all of the rabbits over here.

So you're going to have to ask the press themselves to engage in a serious discussion with you because I hope that they weren't. There still is a bit of reluctance to admit that all of this is going on and they didn't catch it. But I think that that is slowly beginning to change.

Donahoe: So since you're here at Stanford, I want to ask you to direct a few words of advice to the students here.

Stanford has been the birthplace of so many new technologies, former President Hennessy is here today, and he did so much to create a culture of innovation. But many of us are worried about the loss of optimism and the darkening mood around the world of innovation and new technology.

Our current president Marc Tessier-Lavigne is also here, and I had a conversation a couple of weeks ago where we discussed a new imperative for Stanford, to become recognized as the place where the ethical challenges and governance challenges that flow from technology are tackled.

So I want you to speak to the students and describe to them what you would hope for from them, as we try to tackle these divine challenges of hate, polarizing speech, disinformation, or any other ethical issues that flow from technology, either related to the future of work, or governance, or AI, what would you say to the students here?

Secretary Clinton: Well I would hope and maybe implore you to keep in mind the kind of value, that questions and ethical considerations that have to be now part of the debate about the consequences of technological advances.

As I said in my remarks, there are so many reasons to be optimistic and confident and when balanced technology has been such a gift to people, in every walk of life, but we are getting to the point where many of the ideas on the horizon will have far reaching economic, social, and political consequences.

You know driverless cars are really an exciting and neat idea, but what happens to everyone that drives cars and trucks. What are the economic consequences for them? And maybe that's not technology's responsibility but it has to be somebody's to think through, what happens.

Artificial intelligence, there's great raging debate going on right now amongst technological leaders, those that think it is not just a net but an overwhelming positive for humanity vs those that are saying wait a minute, slow down, we don't really understand the consequences. Someone has to help organize that debate, to be a referee, an umpire, you know try to get the smart people that are on the cutting edge of technology to stop long enough and listen to what the consequences might be.

So maybe there are steps that could be taken in order to avoid serious and quite threatening scenarios that I hear about from, you know like, Gates and Musk, and Hawking and others, and you can say they may be wrong but you can't say that without delving in to what their very well educated opinions might be. And same on the other side.

So as students and professors here at Stanford I think you have a tremendous opportunity and obligation to help deter that debate and make it clear that there has to be a value to laden analysis as well as a technological one.

What you're doing here with this initiative is a very good start and sends a signal about what we should be expecting from each other. And obviously it isn't just in areas like AI and driverless cars there are huge implications for biology and for health and education and so much more.

And I guess we should also look for ways to have widely accepted standards for measuring understanding, what are the metrics for the positive and negative understanding. And that's certainly above my pay-grade. But there are a lot of people here that could begin that processes.

You know like developing the Stanford metric model. Something people could use to say okay here are the downsides here are the upsides, what we doing to mitigate them. You know the driver example being a simplistic one with you know real world consequences, for millions and millions of people and their families.

Donahoe: So I'm going to go to the subject of gender. A little risky. This is a topic that continues to present a double bind, where you're dammed if you raise it dammed if you don't, especially in politics, but it's also been an issue here in Silicon Valley. We recently collaborated, on a program NDI here at Stanford, and Filipino activist Maria Ressa, who I think has interviewed you a couple of times, painted a stunning picture about how digital tools are used to incite gender based violence. And this is an intentional strategy of authoritarian leaders to shut down democracy activists that happen to be women. And I would listen to her and it really struck me how her story actually connects to your story. And I would listen to my daughter, and her friends, many of whom are in technology and I would watch them, I would observe how this election has kind of been a wake up call for them. So I wonder, what you think we can do to awaken people to gender dynamics on social media and how it affects political engagement and democratic processes for everybody?

Secretary Clinton: Well, again, how much time do you have?

[Laughter]

Secretary Clinton: I just came from doing a book signing in San Francisco, and signed, I don't know 1,400 1,500 books, about , shook 1,000 plus hands. And the number of women who say,

you know, this election, what happened, is a real motivator for me. I'm an engineer in Silicon Valley, an entrepreneur starting my valley, just determined that I'm not going to be knocked down and set back, because of sexism and misogyny. And I love hearing that because honestly, that's the first step to combatting it.

So I write a whole chapter in the book called, "On being a woman in politics" and I say sexism and misogyny are endemic in society and that's not just in politics, it's in business and the media and its certainly is online, but if we don't talk about it, if it's not polite conversation, or if you're automatically shut down by somebody who either doesn't believe it or doesn't want to engage in it, you know we're never going to change the attitudes and the norms that impact on women and girls and their own ambitions and aspirations.

So look, what we've got to recognize how early girls get the message that they are somehow inferior. You know early research, shows that by the age of 6 girls think they are dumber than boys. They hardly start school, and they have already incorporated that sense of difference, of being lesser, and as young girls get older, face puberty and face society's expectations about what they're supposed to look like and all the rest of it, it becomes even a greater burden, and it becomes even easier to try to avoid it and hide behind it, rather than confront it. And obviously, there's a period of time when in their early 20s, college educated girls, young women by now, make the same amount of money as their peers going into the industry. And that lasts up to 5-7 years and then it stops. And they begin to fall down in the income even if they have the same evaluations, even if they have the same, or in some instances, better education and experience, so by the time they are in their early 30s the gap has widened. And I really applaud the couple of companies here in Silicon Valley that were willing to take a hard look at their pay data and were surprised! You know remember talking Marc Benioff, he was surprised, he thought by no stretch was his company was discriminating between male and female workers, who were of the same education, the same experience, the same time with the company, same type of job description, and he found out they were. And it just is so embedded in sort of the stereotypes for expectations.

The percentage of women getting degrees in computer science from Stanford and every other major institution has dropped precipitously since 1980. Now did young women coming of age starting in 1990 decided that they didn't want to do it. No they were being sent messages that maybe it just wasn't for them or maybe it would be difficult or they were you know even overtly being subjected to sexist comments.

This is a big deal problem. And it's especially viewable(???) online, we know about gamer gate, I mean that was unbelievable. The threats that were made against women who were saying hey what about involving more women in the gaming industry and in the games themselves. They were not just threatened but they were threatened online. They were threatened by phone; they were subjected to stalking. And they were just like, okay fine we won't talk about it anymore. Which was exactly the objective! And when you're being threatened, you know I've been threatened a few times, you think to yourself, well maybe it's just not worth it. I don't want to go through that. So when you look online, a woman, who identifies as a woman you notice a lot of handles now are gender neutral, so women are behind them but women are no longer identifying as women so they can't be shot down and attacked as they are on twitter and YouTube as elsewhere. So a lot of groups, a group of my supporters called Pantsuit Nation, which has over a million people.

[Applause]

Secretary Clinton: They had to go private. They had to go private. Because they were so attacked. And the attacks are violent. I mean the things that are said are just horrific. And also just to say, this doesn't just happen from the right it happens from the left too. It happens from the left and the right.

[Applause]

Secretary Clinton: Why? Because we have opinions. Because we're pushy? Because we want to be president?

[Applause]

Donahoe: Ok, so I just want to break one more story as Larry Diamond will come up and ask a few questions.

I want to bring back a memory for you. In your book you talk about the people who took care of hair and make-up so it wasn't a distraction on the campaign trail. So I have this memory when I was in Geneva that placed your global leadership on human rights and digital technology and your hair.

It was International Human Rights Day, 2011, and you came to Geneva to give this groundbreaking speech on LGBT rights. And it may be hard for people here in Silicon Valley to appreciate the extent to which this subject was completely taboo in the international community at the time just 5 years ago. And this was a time that LGBT activists were literally being hung from trees and being murdered for their advocacy. So you came to break that taboo and use your political capital in front of the international community as a champion for human rights and LGBT rights.

Here's the hair part - on this trip, Huma was about to give birth so she couldn't travel to Geneva, and so nobody had made arrangements for your hair. And so you were about to go out there and give this big speech, and you came up to me, you grabbed me by the shoulders, you looked me in the eye, and you said "Eileen, I need your hairdresser."

So we got that arranged the next morning.

But you were literally out to give that speech in front of thousands of people, and it was live streamed, and Twitter just lit up, you were a message thread globally, there was an instantaneous buzz, and half the tweets were saying, "What's up with her hair?"

And so for me, I think of this story as a kind of a bonding story for all women in the public realm, and I hope it provides some humorous reminder of what global leadership actually looks like.

Larry Diamond: Secretary Clinton, a lot of people asked what advice you have for women students who are thinking about going into politics. I think you answered that with, "Please don't assume that they're only going to come from political science."

Some future woman president could be a computer scientist, so there a lot of questions about what we, young people, can do. So I'll ask it in two forms.

What can we do, as individuals to prevent the spread of misinformation, and just more generally, what can we, this generation, do to stop polarization and change the political dialogue?

Secretary Clinton: Well, to start with an observation, it is so important that young people decide, students and in your 20's, that you're going to vote every time you get a chance to vote. That sounds very simplistic. You know, historically that hasn't been the case, but it does take a change in ideas and maybe peer pressure, for people to feel that voting is their responsibility as soon as they are capable, and encouraging other people to do so as well.

Here in California, there being a bunch of Congressional races in 2018 that could help determine what happens to the House of Representatives, I won 7 districts with a Republican Congressperson. So there's a chance that people could run for office, support those running, and people can certainly vote. I think it's fair to say also that how we overcome the divides is really difficult right now but we have to try.

And I would like to see more dialogue online and in person that says, "Hey, you bring your concerns, I'll bring mine, and let's try to sort them out and have a commitment to figuring out what's true and what's not." We can still disagree, and going back to the tax cut, you can argue that you don't believe in it. But there's an argument that goes, "OK, we'll cut the taxes and that'll stimulate growth." But don't do it and lie about how you're paying for it, which is cutting Medicare and Medicaid. Make the case, "We're going to cut Medicare and Medicaid because in the long run we think it's going to be best for society." OK fine, I don't think it's a very good argument, but make the argument. But don't pretend it's something that it isn't. I think that students can be particularly attuned to demanding that people come with their evidence, if you will. You can read a bill, you can see what's in it, you don't have to listen to what someone claims is in it.

I served with a group of people who are still in the Senate, and I watch some of them trying to defend that repeal nonsense, and they couldn't defend it, but they kept hammering, and people need to say, "Wait a minute. I've looked at it, I've read it and an analyzed what it says, and here's what I have to say to that." So being open to dialogue on different approaches, and there are many, but demanding a certain level of factual decision-making as you try to work through what you think would be an appropriate path forward.

Finally, online lies. You know, a lot of what is online is just insult after insult. It's not discourse, it's how many times you can use profanity to try and demean someone who is on the opposite side of an issue. I think there can be a really important effort to say, "Hey, wait a minute." Online we can say "here's what we believe." But don't leave profanity in arguments, come with facts. Step up and tell us why you believe something rather than just pretending that your position is better than mine without being able to defend it. So I think there's a lot that we can do and should start trying to do.

Diamond: So, I think many people in here would love to hear a little bit more about the tools that were used as Secretary of State to modernize American diplomacy and soft power, and our own colleague who served with you as Ambassador to Russia tried to do that in Russia, so maybe you can talk about, since this is also a struggle for values and not just truth and information, how can we modernize American soft power to project our values and fight this aversion, globally in the digital sphere, without resorting to the same tactics of disinformation?

Secretary Clinton: I think that's a really important question. It seems like such a long time ago, but back in 2010, our main concern was the effort by a lot of governments to crack down on the Internet and to build virtual walls to keep information out and to censor information generators not only within a country but also coming from all parts of the world.

Our goal was to stop the effort by some - China, Russia, Iran, and Saudi Arabia and others – to change the rules governing the Internet and defend the norms and to alter them in order to crack down on speech. So, that was our initial motivation in what was behind the speech I gave in January 2010. We moved on from there and tried to figure out how, if governments were cracking down within in their boundaries, how we could do more to protect dissidents and activists.

We had workshops around the world. I went to two of them, where people who were active on women's rights, disability rights, the environment, climate change, were under tremendous pressure and they wanted to use online tools to make their views known, but as soon as they popped up online, they were subject to being tracked down by the nation's intelligence services. So there was just constant threatening about how to best go forward. So we tried to develop some new tools, like the one where you could press a button and destroy your contacts so if you were about to be arrested you could prevent others from being arrested without very sophisticated exploration of your device and they wouldn't find who your contacts were. So we were doing the best we could. Now even those tools, some of the encryption advice we gave, governments starting using them. So everything had a double edge. We were trying to promote our values of free speech and activism on human rights and related matters, and governments were trying to forestall it or actually co-opt it. So it was a cat and mouse and a constant struggle.

Right now I don't think these values are particularly on the priority list for the new administration, and I worry about that. I was talking about the speech I gave about human rights in Geneva, and the United States joined some pretty bad company last week in refusing to vote for a resolution that condemned the threat of death on behalf activists for LGBT issues. I mean, it was beyond shocking, and I didn't see much coverage of it. I follow those sort of things, so I saw it. I used to call leaders to not change their legal code to change the death penalty for being gay or being an activist. If we don't hold the line on some of these fundamental issues of human rights, who will? So I worry greatly that the balance of power on the internet will be even more on the side of repressive governments.

Diamond: Great. If we have more time, I have just two more questions. We debated a lot today about the responsibilities which you spoke to, the imperatives that rise for private sector companies.

We also debated what is the role of government regulations here, and Europe is full of liberal democracies that are rolling down much more assertive paths of government regulations than we have in regards to compulsion or requirements of companies.

What are your views about the role of governments to regulate or compel certain companies to do certain things?

Secretary Clinton: Well you know, I think our traditions, our constitutional protection for free speech, the judicial opinions that have grown up over the last 240 years puts us in a somewhat different posture, to begin with than a lot of our European friends. So I think that this has to be a place that we explore vigorously and quickly. Because I don't have easy answers for it. I think there's a lot that the companies can do themselves, and they need to do them. Even more accountability, more checking on sources of material, you know Mark Warner, who's been really outspoken on these issues was sort of dumbfounded that some of the Russian ads were paid for in rubles. Which you know should raise a question if anyone's paying attention.

[Laughter]

Secretary Clinton: I think there is a lot that the companies can do. Again, I don't think we know enough about what they knew, and when they knew it, and what they were going to do, and that all needs to be sorted out, but again I would remind us that this was so unprecedented it is hard to know exactly what should have been done because it had never been expected of them and it never had been done. But I think that the congress, for different reasons, will take action, if companies don't demonstrate a willingness to really be accountable with internal controls, and disclosure is a must.

You cannot run political advertising and not disclose a source of the funding for it. Given our campaign finance rules, it still is pretty vague, but that at least is a bare minimum. So those kinds of thing should be probably legislative as well as a part of political speech which already has had a history of legislation. But I think we should have an honest debate with the companies, with ourselves, to try to figure out what we need to do. And I understand at this point too Larry, Europe just feels like it has a lot more experience with the incredibly dangerous consequences of hate speech. You know and people in recent years have seen what happened in Bosnia or Rawanda, where hate speech it wasn't online it was on good old fashioned radio and TV, but imagine how much more powerful it would have been online.

These people are killing their neighbors, these people are going to destroy your home. And you know this does have a contagious affect. There's an article in the Wall Street Journal I think in the last day or two, they used to say in the news if it bleeds in leads, now if it's outrageous its contagious. And I think the Europeans are saying we've been down this road. We are not going to let people get off the ground here, the best we can prevent it. That's not our way, but we better find out a way to protect ourselves from the consequences of this kind of hate speech, propaganda, and everything else goes with it.

[Laughter]

Diamond: But they look as well with what's happening in respect to climate change, what's happening with respect to inequality, what's happening with respect to our Dreamers, and the vulnerabilities they face, tolerance, and just on down the line. I don't want to say they are depressed, because there were so many questions here that I presume were mainly from young women students, about advice you would offer young women about running for office, so I don't see resignation, but I do see several questions in essence, what makes you hopeful now? And what can you leave with people here that makes you hopeful about the future of our country and our democracy?

Secretary Clinton: Well I am fundamentally hopeful and optimistic.

You know I end my book my book on a really optimistic note, and I talk about a new organization I started called "Onward Together" to support new young vigorous grass roots groups that are engaged in civic activity, political activity, recruiting candidates because I think that kind of energy coming from people like those in groups—students and a little bit older—really excites me. And gives me a lot of reason to be hopeful. I also, I guess, can't believe that the level of political behavior we are currently seeing, won't be self corrected by us. You know I find that really hard to believe.

You know I don't think that happens by wishing for it. I think it happens by running people for office, making cases, working to build partnerships and networks, you know all of the hard work that goes in to trying to shift the political agenda.

But how often can people put up with being lied to? How often can people feel that what is being said is untrue? Or what is being done is hard to defend? So, I think common sense and shared experience eventually leads people to say, you know we're not going to put up with this we aren't going to let it go on.

And I think for young people in particular, especially if this was your first presidential election, you really can't afford to be depressed because you know the future is more about you than it is about me and there's going to be a lot more elections and if you don't fight against people that are not running our government based on the majority opinions.. And you know obviously not even the majority vote

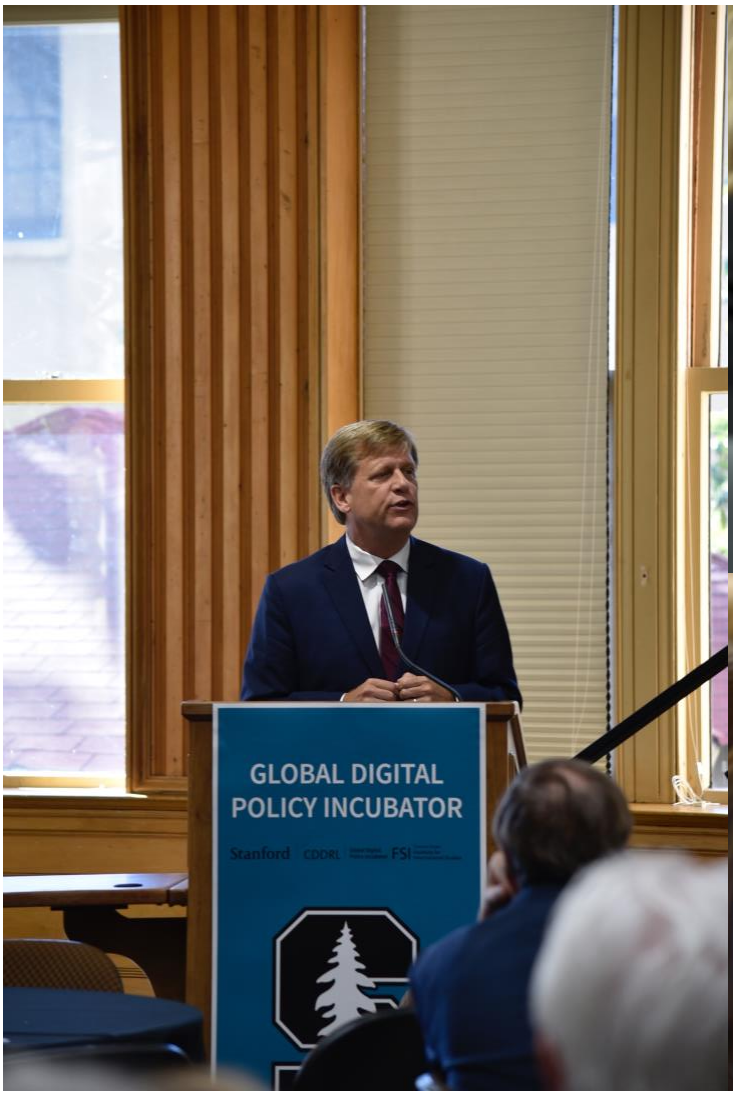
[Applause]

Secretary Clinton: They are making decisions based on minority positions, and look at what happened in Las Vegas. How horrible that massacre was. I'm not saying that one law would have prevented it, but I am saying that sensible gun safety measures would have prevented lot [inaudible]…. And that happens to be the majority position. But the power of the NRA, the total hold it has, on the two major political parties, and I write about this in the book, that it is just astonishing! 90% of American's want to see universal background checks and other sensible provisions. And actually over 80% of people that own guns. And you know 3% of the people in this country own 50% of the guns. 19% own the other 50% of the guns. And we act like oh there's nothing you can do, yes there is you can beat those that being employed fundamentally, not of their constituents, but by the NRA. Our political action can change the political direction.

So if climate change is your issue, or guns are your issue, or immigration is your issue, or if LGBTQ rights are your issue, whatever it might be, decide you are going to be active on those issues and take that action into the political arena, because we need you. We need your voices, and we need your votes, and you know some of you need to move to other states....

[Laughter and Applause]

[END]



Stanford | CDDRL | Global Digital Policy Incubator

FSI *Freeman Spogli* Institute for International Studies