

PROCEEDINGS OF **THE 2019 NIEJELOW RODIN GLOBAL DIGITAL FUTURES POLICY FORUM**

NAVIGATING DIGITAL TRANSFORMATIONS: SURVIVE OR THRIVE?



WELCOME FROM DEAN MERIT E. JANOW



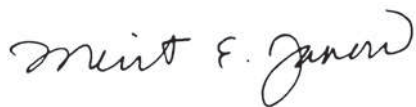
The **2019 Niejelow Rodin Global Digital Futures Policy Forum**, convened on May 10, 2019, by the Columbia University School of International and Public Affairs (SIPA), represented our fifth such undertaking focused on the public policy dimensions of digital technology and its policy consequences.

Similar to previous forums, this year's conference brought together experts from across the University, including scholars from Columbia Business School, Engineering, Journalism, Law and SIPA, as well as a broader community of academics, legal experts, entrepreneurs, journalists and others. This year's theme, "Navigating Digital Transformations: Survive or Thrive?" engaged the broad challenges and opportunities created by wide-ranging digital transformations occurring in the world today.

Unlike past forums, however, a much greater sense of urgency pervaded this year's discussions, reflecting, I believe, a recognition that the consequences of digital transformation are now readily apparent, and the need to identify effective policy solutions has only intensified. Whether it is challenges to privacy and free speech as a result of social media; increasing threats to public or private infrastructure, including election systems; the appropriate regulation of technology companies; governance challenges associated with artificial intelligence; or cyber risk to financial systems, a clear imperative has emerged that more action is needed across the public, private and non-governmental sectors. This year's conference sought to identify key challenges as well as possible solutions.

The discussions were interesting, engaging, at times heated, but deep with insights and suggestions, reflecting the unique perspectives of our panelists from the worlds of media, business, academia, and government. The enclosed proceedings include overviews of each of our six panel discussions as well as two fireside chats. We hope you find them illuminating, thought-provoking, and a basis for further study.

We wish to thank this year's participants for their contributions as well as our partners and collaborators, including the Columbia Data Science Institute, Knight First Amendment Institute, and the Tow Center for Digital Journalism. We also thank the Internet Society for providing streaming support. And we give special recognition to the Niejelow/Rodin family, whose generous support made this year's forum possible.



Merit E. Janow

Dean, School of International and Public Affairs

Professor of Practice, International Economic Law and International Affairs



TABLE OF CONTENTS

Opening Comments <i>by Kara Swisher</i>	1
Session One: <i>Can We De-Weaponize Social Media For Speech?</i>	3
Session Two: <i>Digital Technology and the Future of Elections</i>	7
Session Three: <i>Can We Navigate Major Regulatory Transformations?</i>	11
Session Four: <i>AI & Governance</i>	15
Lunch Keynote <i>with David Sanger</i>	20
Session Five: <i>Global Governance and Cyber Conflict</i>	24
Cybersecurity Fireside Chat <i>with Lt. Gen. John D. Bansemer (Ret.)</i>	30
Session Six: <i>Financial Stability in an Era of Growing Cyber Risk</i>	33
Speaker Biographies	38
Moderator Biographies	46

AGENDA

SESSION 1: Can We De-Weaponize Social Media for Speech?

Social media was meant to be an empowering leap in human communications, allowing citizens to be more connected and creative than at any time in human history. After a decade of rapid growth, global advertising platforms like Facebook and YouTube are commercially successful but civically disastrous. Social media has transformed the public sphere with reckless speed and virtually no regulation. Facebook, YouTube, Twitter and other social platforms are now battling hate speech, propaganda, misinformation and harassment daily. The problem of weaponized speech urgently needs a better response. Can the platforms provide this with technologies and better corporate governance, or do we need legal and policy remedies to safeguard democracy? A panel of policy, legal, technical and practical experts will tackle these questions and discuss what type of reforms are possible, desirable, and necessary.

SESSION 2: Digital Technology and the Future of Elections

The rise of digital technologies and data science pose new challenges for democracies around the world. Democratic elections are under threat from cyber attacks from external actors aimed at interfering with the election process and undermining public confidence in the results. In addition, social media and advancements in communication technology have made it easier to spread disinformation, with the goal of influencing voter behavior. Online manipulation and disinformation tactics, according to Freedom House, played an important role in elections in at least 18 countries from 2016 to 2017 alone, demonstrating the double-sided nature of the internet; with its potential to both enhance and undermine the integrity of our elections and our democracy. The challenges facing the United States are no less acute than in other countries around the world. According to polls, nearly two out of five voters in the United States do not believe elections are fair, and nearly half of those surveyed lacked faith that their votes would be counted accurately. Voter concerns are consistent with widespread reporting on the state of our election infrastructure, aging equipment targeted by external actors beset by a lack of sustained funding. This panel will explore how digital technologies are changing democratic systems and what we can do to address some of the challenges identified.



SESSION 3: Can We Navigate Major Regulatory Transformations?


The policy paradigm has shifted from simply enabling digital technology to how to regulate these technologies. Across the world, governments are passing legislation seeking to protect election and internet security. The implications of regulations may require not just minor changes to technology firms' everyday practices, but also require them to find new business models. Europe's General Data Protection Regulation (GDPR) offers both stronger data protection rules and stiffer enforcement. A German NetzDG law requires online platforms to quickly remove "illegal" content. California, home to some of the world's leading digital enterprises, enacted a broad privacy law that has suddenly prompted legislative activity in state houses across the country and even several federal bills. Faced with merican law enforcement demands to access information held abroad, Congress passed the Cloud Act to manage inter-jurisdictional conflicts over data. Facebook has set aside billions of dollars to respond to an anticipated Federal Trade Communications (FTC) fine. How will companies both large and small fare in this new regulatory world? This panel will assess the opportunity as well as impact of regulation.

SESSION 4: AI and Governance

AI has permeated many aspects of our daily lives—from movie recommendations, targeted advertising, facial recognition, to sentiment analysis. Increasingly, AI systems will be making decisions with wideranging personal and societal consequences (e.g. diagnosing disease, autonomous driving, delivering our packages, determining bail, or detecting terrorists). We will ground this panel's discussion in an understanding of what AI can do today and then proceed to its long-term effects and applications. While the success of AI and its astonishing applications are incredibly exciting, its ubiquity gives us reason to pause. There are several dimensions to policy questions including: Should AI be regulated? If so, what would it look like? Who should be involved in specifying the rules and enforcing them? Does regulation build consumer confidence in AI systems and in the companies that produce them? This session will address these fundamental questions including the use of AI in the US and China. This session will close by looking at AI and governance from a global perspective.

SESSION 5: Global Governance and Cyber Conflict

Conflict in cyberspace—primarily but not entirely between states—seems ever less able to be controlled. In the absence of coherent international law on cyberspace, the U.S. government asserts that it is one of few nations respecting norms of proper behavior. Yet John Bolton, the National Security Advisor, recently remarked that "our hands are not tied" and that the US will "take this fight to the enemy, just as we do in other aspects of conflict." Indeed, some stakeholders would argue that the National Security Advisor's remarks are an admission of U.S. actions all along—that the United States has not been respecting norms. The United States has sought both a secure cyberspace but not so secure that it cannot conduct significant espionage



operations (as revealed by Snowden), cyber-enabled covert action (such as Stuxnet against Iranian nuclear enrichment), and at least the option for strategic and battlefield cyber offensive operations (such as the Nitro Zeus operation planned against Iran). Meanwhile, the underlying technology continues to change in fundamental ways, especially as the Internet of Things drastically increases societal and economic dependence on insecure networks and systems. Cyber attacks which, in the past, might have been ignored or worked around may soon be existential. This panel will address these questions including: What is the mix of individual and collective actions that need to be adopted as the private sector, which creates and uses these technologies, becomes caught in the middle of cyber conflicts and remains an essential partner for global governance? What should be the private sector's priorities, such as resilience, to form a basis for global cyber agreements?

SESSION 6: Can We Achieve Financial Stability in an Era of Growing Cyber Risk?

Since the financial crisis a decade ago, government authorities and the financial sector have been working to improve overall resiliency. Parallel to these efforts, governments and industry have been grappling with increasing cyber risk—increased frequency and sophistication of cyberattacks and an ever-growing reliance on digital technology. SIPA's Cyber Risk to Financial Stability (CRFS) Project examines the gaps and strengthens the intersection of cyber and financial stability community efforts to boost resilience in the financial system. The financial sector is at the forefront of cybersecurity and industry-wide information sharing and collaboration. Over the last few years, institutions have been built to increase resilience within the financial sector—FSARC, the Department of Homeland Security's National Risk Management Center—while research and regulatory efforts have begun to acknowledge and analyze cyber risks to financial stability—at Columbia SIPA, the Financial Stability Board, and the Treasury Department's Office of Financial Research. However, there is more work to be done—for example, there remains a lack of globally coordinated policies and regulations, little understanding of the technology mapping of financial system processes, and how new technologies will impact markets and systems, among other areas of focus. This panel will explore several questions including: Efforts to date in areas of financial stability and cyber risk, reflecting on CRFS' framework. Key areas to prioritize for government, industry, and academia to support efforts. And what challenges may lie ahead including prescriptions for public and private sector to act to further resiliency.



PROCEEDINGS



OPENING COMMENTS

Kara Swisher


*Technology Business Journalist and
Co-Founder of Recode*



Swisher captured the technology landscape of May 2019 by touching upon two significant discussions. In the first, a *New York Times* op-ed, Facebook cofounder Chris Hughes argued that the company should be broken up. Describing the power of Mark Zuckerberg as unprecedented and un-American, Hughes highlighted the growing influence of technology giants over the past decade and the threat they pose to democracy, as evinced by the 2016 election.

Swisher then turned to the second discussion, her interview with Tristan Harris of the Center for Humane Technology. Harris has worked to illuminate the ways in which technology is engineered to addict users, as well as the industry's failure to understand its own power. He argued that technology addiction, polarization, "outrage-ification," and micro-celebrity culture "are not separate problems. They're actually all coming from one thing, which is the race to capture human attention by tech giants." A unified agenda is urgently needed to arrest "human downgrading," the "social climate change of culture."

Drawing on these discussions as well as her own 25 years covering Silicon Valley, Swisher outlined several ideas essential to grappling with the next wave of technology, which will change the world in unprecedented ways.

- 
1. In Swisher's words, "Everything that can be digitized will be digitized"—every job, utterance, and behavior. Given that AI will perform so many tasks better than humans can, this development is inevitable. It remains to be seen what power we can retain.
 2. Though an ostensible meritocracy, Silicon Valley has in fact degenerated into a "mirror-tocracy." A small, homogenous group of young white men, incapable of understanding social ills or the implications of its own work, is reshaping society. Now and going forward, we must look closely at who designs the technology and what values it reflects.
 3. Those behind the technology have neither solutions for the problems it creates nor an interest in engaging with those problems. Technology companies, particularly Facebook and Google, have created giant public-private digital cities that we all occupy. Though happy to collect the rent, they have declined to provide services such as a police force, firefighters, garbage collection, sewers, or signage. We have been left to fend for ourselves and figure out our own path through the problems they have created.

Swisher closed her comments by considering how we might best address these problems. Regulators must get involved, as they have in other industries throughout history. We must work to craft regulation that imposes the necessary guardrails without impeding innovation. Without these guardrails, we are in danger of squandering truly marvelous technology.

SESSION ONE

Can We De-Weaponize Social Media For Speech?

Kara Swisher

*Technology Business Journalist and
Co-Founder of Recode*

John Battelle

*Senior Research Scholar, Columbia SIPA,
and Co-Founder and CEO of Recount
Media*

Alexander Macgillivray

*former General Counsel, Twitter, and
former Deputy U.S. CTO*

Jameel Jaffer

*Director, Knight First Amendment Insti-
tute, Columbia University*

Emily Bell

*Tow Center for Digital Journalism, Colum-
bia Journalism School (Moderator)*



Background

Social media was meant to be an empowering leap in human communications, allowing citizens to be more connected and creative than at any previous time in human history. After a decade of rapid growth, global advertising platforms like Facebook and YouTube are commercially successful but civically disastrous. Social media has transformed the public sphere with reckless speed and virtually no regulation. Facebook, YouTube, Twitter, and other social platforms are now battling hate speech, propaganda, misinformation, and harassment on a daily basis. The problem of weaponized speech urgently needs a better response. Can the platforms provide this response through technologies and better corporate governance, or do we need legal and policy remedies to safeguard democracy?

Panelists

In the first session of the Forum, a panel of policy, legal, technical and practical experts discussed what type of reforms are possible, desirable, and necessary.



Innovating the Business Model

A consensus quickly emerged that legislation limiting what people can say on social media is not a viable solution. Macgillivray emphasized that, while even controls on speech are tolerated, a federal acceptable speech commission or decency principle applied to all online speech would impinge on rights to liberty and progress and result in the majority persecuting and silencing the minority.


Jaffer pointed out that regulation limiting free speech would effectively replace Mark Zuckerberg's control over the speech environment with that of Donald Trump, and that the courts would strike down any legislation that limited free speech beyond what is permissible under the First Amendment. However, he offered the caveat that not everything social media companies do is properly thought of as speech protected by the First Amendment, and that much can be done by way of regulation without running afoul of it. While acts of censorship like Facebook kicking Alex Jones off the platform have drawn attention and incited debate over who should be allowed a voice in the public square, this perhaps distracts from a bigger question: why is Alex Jones so popular on Facebook? Jaffer argued that Jones's popularity stems not from persuasiveness, but rather the way Facebook privileges certain types of speech over others. He urged attention to the algorithmic decision-making that ends up "amplifying the worst speech and suppressing speech we actually need."

The algorithms and business models underlying social media platforms were a major concern throughout the panel. Battelle linked the advertising business model to the engagement metric. Rather than an inevitability, this model was simply the one that came out on top. As a result, three or four basic inputs of engagement drive division, polarization, and enagement. CEOs may express regret over prioritizing likes, follower counts, and other engagement metrics, as Twitter's Jack Dorsey recently did. But while it is within his power to change how these inputs effect the algorithm, there is little chance he will do so, given that the metrics are now intrinsic to the business model and that Twitter is a public company with shareholders.

For Battelle, the direct connection between model and outcome is clear but deeply underdiscussed, with major speech problems emerging from the need to drive advertising and profit. He argued that while "unbridled steroidal capitalism" is at the heart of the problem, the solution is not decommercialization, but instead fostering an environment where competitive companies can gain traction with new models. Building this environment will not be easy, given the reluctance of venture capitalists to support challengers to the current social media giants and the complacency arising from the assumption that search and e-commerce problems have all been solved. Yet there is some reason for optimism as vulnerabilities and opportunities become apparent. Significant progress may require new incentive structures that encourage innovation, making this a problem for economic policy.

Diversity and Power Structures

Swisher agreed that, while Silicon Valley may pretend at shock, the system works exactly as it was built to. She cited the work of Nicole Wong, former Deputy U.S. CTO, which emphasizes the importance of careful and



deliberate algorithm architecture prioritizing accuracy, community, and context over speed, virality, and engagement. For Swisher, the architecture of the major social media platforms reflects the absence of diversity in Silicon Valley, where those in positions of power have little or no experience being marginalized, unsafe, or unable to speak up. Macgillivray noted that, because these experiences are difficult to learn through observation, companies cannot change simply by educating current employees—they must become more diverse. He saw progress in the move away from “manels,” panels made up entirely of white men, but lamented that board membership remains largely unchanged.


Jaffer cautioned that simply swapping in people who have first-hand experience with marginalization for those who do not may be insufficient to address speech problems that are structural in nature. Swisher agreed that this is the case when boards serve as little more than advisory groups or occasional dinner companions for CEOs, claiming to protect them from Wall Street investors or short-term thinking rather than pressuring for improvements. As an example of a CEO in whom too much power is concentrated, she cited Zuckerberg’s undermining of accountability out of a reluctance to fire anyone. Swisher argued that one person, “the King of Facebook,” should not be in charge of “every single decision for the most important communications platform in history.” Because company founders and venture capitalists prefer such power structures, they have continued in recent IPOs. Macgillivray saw something of a silver lining in the growing field of academics and content moderation professionals now providing input from outside companies. But while this development is necessary, it is not sufficient.

Privacy, Transparency, and Individual Agency

The panel saw it as implausible that the major platforms would ever be de-privatized and dismissed antitrust action as neither the most effective potential solution nor likely to occur. Jaffer raised the possibility of breaking up Facebook by separating the social network from the interface. Macgillivray recommended the work of Daphne Keller of the Stanford Center for Internet and Society on models within communications law for speech-related antitrust and emphasized the importance to how we think about antitrust of including data and networks within acquisition valuation.

Fordham University law professor and 2018 New York attorney general candidate Zephyr Teachout tweeted to the panel suggesting a ban on targeted advertising. Swisher regarded such a tactic as unlikely to succeed, given the platforms’ near-total immunity. She did float the idea of threatening to repeal Section 230 of the Communications Decency Act, which protects the platforms from liability for user content, to see what would happen.

The panel regarded privacy regulation as more promising route forward, including rules regarding what information platforms could collect about users or how that information could be used. Transparency regulation could require the platforms to disclose how their algorithms make decisions, although, as Battelle observed, even the platforms themselves may not have full information about what they’re doing. He suggested disallowing terms of service that restrict journalists and researchers from using digital tools to study platforms.



Battelle went on to discuss what he calls the “Shadow Internet Constitution,” which governs how our information flows through society. We agree to this Constitution continuously by consenting to various terms of service with little understanding of their contents or implications. They often prohibit machine readable data portability; Battelle believes that empowering users to efficiently and easily transfer their own data from one platform to another could solve a fair number of problems.

The question of user agency was raised again later by an audience member, who wondered about the potential efficacy of public education about data trails. Drawing a comparison to warning labels on cigarettes, Battelle agreed that users don’t understand what they’re in for when they engage with these platforms and that an educated public would be a step forward, but cautioned that regulation is also needed to limit what information companies can collect. Swisher highlighted the addictive qualities of the platforms and suggested that regulation could limit or make transparent their manipulative tactics.

Conclusion

Ultimately, this panel revealed the weaponization of online speech to be a complex set of problems with no single solution. Macgillivray pointed out that solving one problem may exacerbate another. Taking harassment as an example, he explained that methods employed to give white supremacists a way to understand they are unwelcome, such as disinformation and doxing, may themselves closely resemble harassment. This tension between solutions is also apparent as more closed systems emerge and platforms pivot towards greater privacy, providing enclaves remote from academic or journalistic study for groups like white nationalists. As Jaffer observed, in this case, the problems of centralization are traded for those of decentralization.

The panelists anticipated major developments in this arena in the coming months and years. Swisher highlighted the critical importance of new developments in New Zealand, Australia, and Europe, as well as U.S. states developing their own privacy laws (and the potential for conflict between those laws). Battelle noted the prominence of issues like data protection, privacy protection, election interference, and an Internet bill of rights in the talking points of the Democratic presidential candidates. He expressed approval of the place of these topics in the national dialogue, if also skepticism that they would be addressed with nuance. The discussion concluded with Macgillivray observing that our society has not yet discovered a way to connect everyone as one big community, and Battelle suggesting that this goal was perhaps ludicrous to begin with.

SESSION TWO

Digital Technology and the Future of Elections

Josh Benaloh

Senior Cryptographer, Microsoft Research

Renée DiResta

Mozilla Fellow, Media, Misinformation, and Trust

Mac Warner

West Virginia Secretary of State

Avril Haines

Deputy Director, Columbia World Projects (moderator)



Background

The rise of digital technologies and data science is posing new challenges for democracies around the world. Democratic elections are under threat from cyberattacks from external actors aimed at interfering with the election process and undermining public confidence in the results. In addition, social media and other innovations in communication technology have made it easier to spread disinformation and misinformation, potentially influencing the way citizens vote. Online manipulation and disinformation tactics, according to the Freedom House, played an important role in elections in at least 18 countries from 2016 to 2017 alone, demonstrating the capacity of the internet to both enhance and undermine the integrity of democracy and elections. These challenges extend to the United States, where polls have shown that nearly two out of five voters doubt elections are fair, and nearly half of those surveyed lacked faith that their votes would be counted accurately. These concerns perhaps reflect widespread reporting on the state of U.S. election infrastructure, which includes aging equipment, has been targeted by external actors, and lacks sustained funding.

Panelists

Two key topics in election interference, voting mechanics and voter manipulation, relate to different areas of expertise and so are often discussed in separate silos. The second panel of the Forum attempted to bridge these two topics, with panelists exploring how digital technologies are changing democratic systems and what we can do to address some of the challenges identified.

Registration and Voting

Two contrasting perspectives on the security of voting mechanics emerged from the panel. Warner saw U.S. elections as fundamentally secure and the narrative of their vulnerability as exaggerated and inimical to voter confidence. He framed the problem as one of body, mind, and spirit: the body (the mechanisms of voting and tabulation) is sound, the mind (processes such as registration) is somewhat afflicted, and the spirit (trust in the electoral process) is most imperiled. Warner emphasized that although the Internet creates vulnerabilities for registration systems, those of only three states have been hacked, and there is no evidence that Russian hackers changed a single vote or compromised tabulation in 2016.


For Warner, the decentralization of U.S. elections, with each state ensuring the integrity of its own results, is a strength. Rather than targeting a monolith, hackers must go after 50 separate systems. By treating election infrastructure as critical to homeland security and imposing greater control, the federal government could inadvertently erode this strength. Warner suggested that a better step would be for the federal government to more readily disseminate information about potential threats.



Renée DiResta and Mac Warner

While Benaloh agreed that there is no evidence that any votes were changed, he cautioned that the technology related to casting and counting votes is alarmingly vulnerable, citing University of Michigan computer science and engineering professor J. Alex Halderman's claim that his undergraduate security class could have changed the results of the 2016 election. Further illustrating this vulnerability, he pointed out that there are 8,000-plus U.S. jurisdictions; expecting a local county or township IT department to block the efforts of a foreign nation-state is simply unrealistic. Benaloh believes that there's much we can do to make elections more secure, but also that they will never be impervious to attack.

These distinct views crystallized once again on the topic of mobile voting. Warner prioritized making it available to active overseas members of the U.S. armed services, only 13% of whom vote and have their votes



counted. He saw the chance of hackers accessing the mobile system as too remote to preclude its use for this narrow group.


However, Benaloh stressed that there are tremendous security vulnerabilities inherent to returning completed ballots online, called mobile voting without end-to-end verifiable technology “unconscionable,” and did not recommend its use in any context at this time. He further described blockchain voting as “just a terrible idea” that would introduce new problems and make things worse. Blockchains don’t address any of the key problems in online voting: authorization to vote, anonymity and confidentiality of the process, and verifiability. In his opinion, anyone promoting blockchain voting is dishonest or else misunderstands blockchain application or voting. Benaloh also pointed out that early studies have suggested that, perhaps counterintuitively, the availability of Internet voting does not actually increase voter participation. It’s not obvious, then, that mobile voting is a crucial step for enfranchisement.

Manipulation and Disinformation

DiResta outlined the social influence campaign conducted by the Internet Research Agency, a third-party contractor with extremely strong ties to the Russian government. Over several years, the Internet Research Agency worked to divide America into tribes, solidify feelings of pride, and convince members of different groups of how they should feel and vote. On both the left and the right, it built and reinforced cultural bonds. These highly sophisticated efforts demonstrated an understanding of how to inflect messages to best reach and sway voter subgroups. For example, rather than treating the right as a monolith, the campaign targeted the young right with meme culture and the older right with Reaganite nostalgia for an America that used to be.

DiResta went on to explain that the Internet Research Agency actively infiltrated communities by hiring influencers and giving them resources for around 81 in-person events that would create a spectacle and be broadcast via the media. In essence, it conducted a spying campaign, recruiting Americans to unwittingly serve as agents of a foreign power. It also disseminated misinformation, such as supplying members of the Latino community with incorrect polling places, or claiming that Democrats who voted for Bernie Sanders in the primaries could not vote for Hillary Clinton in the general election. It discouraged certain voter groups, as when it propagated the message that Black Americans did not like and should not support Clinton.

While DiResta saw significant evidence of engagement with this content, she explained that it is impossible to know whether it flipped the election. Its effects reverberate still, with members of targeted communities continuing to share it. This raises several challenges: What can we do when foreign propaganda resonates with Americans? How can we dampen social media amplification when it’s impossible to catch and shut down the fake accounts before they seed divisive content? DiResta raised the possibility of platforms slowing virality, though noted that this might be criticized as censorship. Because the First Amendment makes us wary of a false positive silencing someone, democracies are disproportionately vulnerable to such manipulation. This allows the content to stay up longer than it should and go viral, while corrections never go viral—some percent of the population will continue to stand by the content. The result is an “information laundering ecosystem”



characterized by distrust of the information we receive and unease when so much effort is required to figure out what is real. Rather than mining diverse sources for information or engaging in discourse with other citizens, we entrench more deeply in our silos. As Iran and other actors begin to employ the same tactics, we must find ways to harden the social information environment.

Restoring Public Confidence

Benaloh highlighted the importance of election auditing, which can prove the absence of tampering after an election with near-perfect certainty, to restoring trust in the democratic process. He described two principle auditing mechanisms. Risk-limiting administrative auditing involves randomly picking precincts and checking ballots against expectations in efficient and dynamic ways. End-to-end verification allows individual voters to check for themselves that their votes have been properly recorded rather than depending on the courts to allow recounts. Microsoft is partnering with Columbia to build and improve both types of tools.

Warner expressed optimism about current pre-election voting machine testing and postelection audits, but allowed that the system could be better still. He applauded the efforts of the MS-ISAC and the bipartisan Defending Digital Democracy project at the Harvard Belfer Center. He urged the need for education to make voters better at spotting propaganda and, above all, unity, framing election interference as neither a left nor a right problem, but an American problem.

Echoing Warner's hope for an end to President Trump's avoidance of this topic out of a sense that it calls his election into question, DiResta explained that many Trump supporters are unable to accept that election interference occurred because it is so closely linked in their minds with collusion. She noted that while early interference was relatively sloppy and easy to detect, with attributable VPNs and Twitter accounts registered using Russian phone numbers, it has grown subtler. However, social media platforms have grown more aware of the problem, and public-private partnerships are emerging. We now have pipelines in place for reporting suspicious content to relevant researchers within social media platforms, the FBI, or other government agencies. Experts in the field are working to develop more robust detection frameworks that hinge on dissemination and distribution patterns rather than narrative, to lessen the risk of individual bias.

SESSION THREE

Can We Navigate Major Regulatory Transformations?

Victoria Espinel

President and CEO, BSA|The Software Alliance

Eli Noam

Paul Garrett Professor of Public Policy and Business Responsibility Economics, and Director, Columbia Institute for Tele-Information

Samm Sacks

Cybersecurity Policy Fellow and China Digital Economy Fellow, New America

Fred Wilson

Partner, Union Square Ventures

Tim Wu

Professor of Law, Science and Technology, Columbia Law School

Anupam Chander

Professor, Georgetown University Law Center (Moderator)



Background

The years of enabling digital technology have given way to those of regulating such technologies. Around the world, over 130 governments have established data privacy regulations. These rules generally seek to protect election and Internet security as well as copyright holders. Europe's General Data Protection Regulation (GDPR), adopted in April 2016, strengthens data protection rules and establishes harsher penalties for noncompliance. The German Network Enforcement Act (NetzDG), passed in June 2017, requires online platforms to quickly remove "illegal" content. California, home to some of the world's leading digital enterprises, enacted a broad privacy law in 2018 that has prompted a flurry of legislative activity in other U.S. state houses and even a number of federal bills. Faced with American law enforcement demands to access information held abroad, Congress passed the Cloud Act in March 2018 to manage inter-jurisdictional conflicts over data.

Much of the debate surrounding regulation has focused on Facebook. In the days leading up to the Forum, Singapore passed new legislation to force online platforms to police fake news. *The New York Times* published an opinion piece by Facebook co-founder Chris Hughes arguing that the social media platform has grown too powerful and should be broken up.

Facebook spokesman Nick Clegg, formerly Deputy Prime Minister of the United Kingdom, responded “you don’t enforce accountability by calling for the break-up of a successful American company.” Two months after the Forum, the U.S. FTC fined Facebook an unprecedented \$5 billion for privacy violations.

To meet new requirements, technology firms like Facebook may need to go beyond minor changes to their everyday practices and instead reinvent their business models. The implications of these regulations are as yet unknown and in flux.

Panelists

In the third session of the Forum, a panel of academics, venture capitalists, and policymakers assessed how companies both large and small will fare in the new regulatory landscape.

Assessing and Adapting the GDPR

Close to a year after implementation of the GDPR in late May 2018, the panelists took stock of its strengths and weaknesses and considered whether it is—or ought to be—the de facto global norm. After heavy involvement in the debate surrounding the crafting and ratification of the GDPR, stakeholders have experienced few surprises over its realization. For some, the GDPR represents a necessary, if imperfect, step towards global norms. It harmonizes standards across Europe and brings us closer to universal harmonization of rules pertaining to privacy, data localization, digital trade, and cybersecurity, which will hopefully be established over the next five to ten years.

Some panelists, however, questioned the efficacy of GDPR in protecting individuals’ privacy and criticized its reliance on the user consent model. Others saw deeper flaws, going so far as to describe the GDPR as “both procedurally and substantively a poor piece of legislation.” The procedural critique sees Europe’s insistence that the world abide by the GDPR as imperialistic, and the process of reforming or adapting the regime as onerous. Potential substantive flaws include the right of access to information, which allows those who illegally acquire basic identifiable information about other users to access sensitive personal data.



Anupam Chander, Fred Wilson, and Victoria Espinel

Even assuming that GDPR is effectively drafted, questions remain over whether it ought to be “cut and pasted” into U.S. law. For small businesses, this approach may be preferable to avoid the costs and difficulties of complying with multiple regimes. A potential alternative solution lies in drafting laws that are interoperable with the GDPR but grounded in the U.S. common law tradition rather than a civil legal system. Such laws would need to be crafted carefully to avoid stranding companies in the middle of the two regimes.

The Chinese Model

The panel also considered China as a pioneer of Internet regulation and asked what lessons might be learned from it. China studied the GDPR as a model for its own regulations, which it quietly put into effect the same month as the GDPR. This vast regime addresses online content, critical infrastructure, and supply chains. It emphasizes personal data protection; a massive audit currently underway could result in the revocation of the business licenses of apps found to have collected excessive personal data.

This undertaking may seem difficult to reconcile with China's reputation as a surveillance state. It helps to recognize that its emphasis is on data protection rather than privacy. Different rules apply to the government, which is cracking down on Chinese Internet companies that have become powerful by amassing data. The major competing platforms further increase their power, to the point of rivaling certain government ministries, and control the next wave of technology by aggressively buying up startups. This push-pull undermines the narrative of Chinese companies always doing the bidding of the government. The Chinese government simultaneously helps companies succeed with its support and backing and, although unlikely to break them up altogether, uses regulatory tools to keep them in line.

The Chinese government, panelists pointed out, has voiced its opposition to cryptocurrencies yet allowed them to flourish. This may be inadvertent, or a manifestation of the “move fast and break things” attitude essential to the early success of the Internet in the United States. The U.S. government claims to espouse the opposite attitude towards cryptocurrencies, yet has greatly checked the growth of this sector; 80%–90% of all crypto trading and transaction volume now occurs in Asia, predominately in China. U.S. regulatory policy, Wilson argued, has allowed China to co-opt the next great tech sector. These dynamics matter because, as Sacks pointed out, geopolitics is playing out largely in the digital realm. Rivalries between the United States and China now go beyond military and GDP to encompass global technological influence, innovation, and reach in markets around the world. We are in the midst of a great technological power rivalry.

Antitrust

Instrumentalizing this rivalry, Facebook has argued that excessive U.S. regulatory interference would create a power vacuum that Chinese companies would seize. Wu found it bold of Facebook to position itself as the champion of the United States, and saw it as aspiring to effectively become the regulated monopoly of social networking—“the AT&T of sociality, forever.” He positioned his argument historically, referencing a similar dilemma, when AT&T and IBM, then the most powerful technology companies in world, claimed that antitrust enforcement against them would effectively hand over the future to Japan, where the industry prospered with the support of a brilliant and magnanimous government. The U.S. government disregarded this warning, to the long-term health of its technology economy; Wu believes that by turning on its champions and forcing them to face competition, the U.S. government forces companies to either toughen up or be replaced by something better. Antitrust serves a constitutional function as a final check on private power, when a company becomes so powerful it is essentially government and cannot be dislodged in any other way.

Noam highlighted the danger of giving law enforcement the power of deciding whom to target for antitrust violations. Wilson went further, insisting that antitrust is inherently capricious and political, and that applying the same rules to all companies can level the playing field and increase opportunities for new competitors to enter the fray. He argued that breaking up a company may not be the best way to create more competition. The market may benefit more from forcing companies to allow customers to do what they want with their data. Data portability, allowing third parties API level, machine readable access to customer data, would increase competition. This differs, however, from compulsory licensing, forcing companies to turn over data regardless of what the customer wants. Data portability could be tied to user ownership of data and freedom to revoke the rights to it or to sell them to a third party.

Conclusions

The panel concluded by noting that each regulatory regime has its strengths and weaknesses and cautioning against romanticizing those of other countries. A regime that works well in one context may not be applicable to another, making it unlikely that any single regime would be perfect or effective for all countries. A better approach may be to strive towards consensus on certain fundamental issues, with the particulars tailored to specific markets—“regulatory floors as opposed to regulatory ceilings, and variation across the world.”



Victoria Espinel

SESSION FOUR

AI & Governance

Ronaldo Lemos

Director, Institute for Technology and Society of Rio de Janeiro, and Visiting Professor, Columbia SIPA

Daniela Rus

Director, Computer Science and AI LAB, MIT

JoAnn Stonier

Chief Data Officer, Mastercard

Eric Talley

Professor, Columbia Law School

Jeannette Wing

Director, Data Science Institute, Columbia University (moderator)



Background

AI technology already pervades our daily lives. It is used in movie recommendations, targeted advertising, face recognition, and sentiment analysis. More and more, we will see its use in making decisions about people with life and societal consequences, e.g., diagnosing disease, driving our cars, delivering our packages, determining bail, or detecting terrorists. While the success of AI technology and its astonishing applications are incredibly exciting, its very ubiquity gives us good reason to pause.

Panelists

In the fourth session of the Forum, a panel of legal experts and technologists representing both academia and industry evaluated whether AI should be regulated, what that regulation should look like, and who should formulate and enforce the rules.

The Current State of AI

Rus began the discussion by outlining the current capabilities and limitations of AI and data science technologies. Twenty years ago, the idea of pervasive computing was a pipe dream; now we barely notice the amount of computation in our daily lives. We are on the brink of another major shift, this time with AI. “AI” is a broad term used to refer to three sub-

fields of computer science: artificial intelligence, machines with human-like characteristics in how they see, communicate, move, and learn; robotics, computation put into motion; and machine learning, a combination of robotics and artificial intelligence that uses data to find patterns and make predictions. AI has the potential to provide us with personalized healthcare, prevent car accidents with automated driving, transport goods with less environmental impact, keep information safe, take over routine tasks, and leave us more time to exercise expertise and critical thinking. Every field that uses data is likely to benefit.




However, there are still significant limitations to machine learning. While machines excel at finding patterns, they only become useful after training with massive amounts of data that humans have labeled. The machine is only as good as the data that trains it, and errors or biases in the data will impair its performance. Moreover, the machine does not provide an explanation along with its answer, complicating the interpretation of its decisions and creating a need for regulation. Other challenges in this space include expanding its province beyond experts, remedying the ease with which systems can be fooled, and reducing the vast quantities of data required for training. Machine learning is about finding patterns in data, predicting what might happen, and suggesting action items, but these operations are currently fairly low-level.

In the future, these deficiencies may be addressed by introducing deep reasoning, making systems more “human-like.” Future developments will hopefully include greater explainability and interpretability and an expansion of privacy protection with systems that learn and compute using encrypted or aggregated data.

Formulating AI Regulation

Citing the use of machine learning engines in court systems and government agencies to make decisions about people and the recent call from Brad Smith, president of Microsoft, for regulation of facial recognition technology, Wing turned the conversation to regulation. Stonier explained that, although many national and supranational organizations have AI taskforces addressing ethics and accountability, regulation has not yet emerged. This is in part because AI is still in very early stages and can be used in different ways across many different contexts. Facial recognition, for example, involves AI that is deeply personally impactful; weather prediction AI may draw on the same amount of data but is not nearly as personally impactful. Should the same regulation apply to both?

Stonier emphasized the need for carefully crafted regulation. Faced with the convergence of technology and law, regulators will need to understand facets of the vast amount of data input to train systems including



accuracy, lineage, and veracity, as well as the ways algorithms monitor algorithms, and the ways individuals partner with the technology to observe what decisions it's making and diagnose whether any problems emerge from flaws in the model or the data. Effective regulation cannot be crafted at some high level. Regulators must instead sit down with data scientists who have a deep understanding of AI. Responsible companies must also participate, disclosing their own AI-related processes and results to help build regulation that makes sense for society. Already, corporations like Mastercard are working with data scientists on voluntary frameworks and assessing how to enact responsible information practices and navigate the world of governance around AI. Even though it's still early days for AI, this work must begin now, as it will only get more difficult as systems grow more capable.

The Intersection of AI and Law

To understand what it would mean to regulate AI, the technology community is looking to policymakers and the legal community. Talley raised two major questions about AI and law, starting with: how should the legal system think about regulating AI and its uses within industry? In recent years, privacy issues have dominated discussions around regulating the industry and actors that use AI technologies, with large actors struggling to ensure the integrity of their own privacy protection systems. While the law has a set of ground rules or general principles about privacy, more work is needed to determine what objectives we are attempting to accomplish through privacy. We must also consider, especially in the financial services industry, how algorithms might draw on decision-making criteria that has already been deemed impermissible. Discriminatory bias may creep in even if information such as race, age, gender, or sexual orientation has been excluded from datasets, since the model could latch onto close correlates instead. AI can run up against protected classes in other ways as well. For instance, iPhones are capable of detecting minute vibrations and oscillations in a user's grip, a potential early marker of Parkinson's disease. By gathering this information, Apple could unwittingly be using a protected class to make predictions.

Talley then turned to his second major question: how will AI change substantive law, courts, and the administration of justice itself? There's a fear that the court of tomorrow will consist of essentially no humans (apart, perhaps, from the defendant). This prediction echoes the fable of the law as essentially an engineering system built on complex rules; mastering the rules is the same as mastering the law. Based on their own educations and expertise, computer scientists may find this fable appealing. This framing is problematic because any set of rules will be woefully overinclusive or underinclusive. Rules can contradict one another or leave too much on the table. The legitimacy of law hinges on more than consistency. The application of legal standards must also make sense from policy and normative perspectives, which are not static. The law, then, is adaptive. The most famous cases are those that broke with pre-existing patterns, pushed the law in new directions, and cast matters in a new light. AI with enormous predictive capabilities based on historical legal data may be of little use when normative commitments shift.

As AI penetrates everyday life, it will necessarily change how we think about legal structure. As an example,

Talley discussed the interaction between autonomous vehicles and human cyclists and pedestrians. This is a hard problem that will force us to rethink product liability, negligence law, and product regulation, and trigger dramatic and rapid change in the current model of automobile law. As autonomous vehicles grow safer, the cost-benefit analysis for pedestrians and cyclists may shift, leading them to take more risks. It may not be possible to predict now how people will behave in the future in response to autonomous vehicles—we will have to adapt to the adaptations.

AI Regulation and Emerging Markets

Lemos drew on his experience developing an Internet of Things national plan for Brazil to explore how AI governance will take shape in emerging economies. To illustrate that this is a question not for the future, but for now, he described a chatbot used by the government of São Paulo to interface with citizens. This automation has introduced new efficiencies, but many people do not realize that they are interacting with a machine. There has been little discussion of how this AI should be governed.

In the developing world, problems with data extend beyond its proper usage and regulation to, in some cases, its absence. This dearth can create blind spots and gaps, making the AI stack imperfect. In Rio de Janeiro, Google Maps shows green spaces such as parks in the place of favelas, or shanty towns. Deep fakes are also a problem. In Brazil's last election, a compromising video of a governor went viral. The video is unclear, and its authenticity is the subject of conflicting expert assessments.



Eric Talley and Ronaldo Lemos

The existence of flawless video and image forgeries has left voters in a state of doubt, and has the potential to spread disinformation and interfere with elections.

Determining which laws apply to AI in Brazil involves examining the legal system to assess what regulates the cloud, outcomes, consumer protection, and explainability. Before attempting to change the law, it is necessary to put all these pieces together. Only then does it become clear whether more laws are needed, or whether some laws need to be dispensed with.

Lemos deemed Brazil's multi-stakeholder approach to AI governance a success. He emphasized that states cannot do this alone. They must build coalitions with the private sector, NGOs, and the scientific community. Lemos synthesized a point raised by most every panel member: this is not an issue that can be solved by regulators alone, or technologists alone. Without collaboration, AI governance simply will not work.



China

The panelists touched upon the development of AI in China. Rus observed that China's AI has advanced rapidly, spurred by ambition, agility, huge resources, and a government plan to surpass the AI of other nations by 2025. Because China has fewer data regulations and concerns, technologists have access to much more data. This has led to better-trained products, resulting in more revenue, resulting in more engineers, in an ongoing cycle. China's AI publications, patents, and relative company valuations are quickly drawing even with those of the U.S.

Stonier also remarked on China's data policies. China has set itself up to use all the data inside its own economy to enable innovation, and the government has set up a society where all the data is available for training, leading to a large pool of highly skilled data scientists. She emphasized, however, that different governments have different advantages for different societies. No one government has a clear advantage yet. Instead, innovation of different kinds is springing up in various countries. As time goes on, we will likely see a convergence on data regulation policies, with certain baseline principles enacted.

LUNCH KEYNOTE

David Sanger

National Security Correspondent for The New York Times

In conversation with:

John Battelle

Senior Research Scholar, Columbia SIPA, and Co-Founder and CEO of Recount Media

Merit E. Janow

Dean of Columbia SIPA




Merit E. Janow, David Sanger, and John Battelle

Over lunch, keynote speaker David Sanger, National Security Correspondent for *The New York Times*, responded to questions from John Battelle, Co-Founder and CEO of Recount Media, and Merit E. Janow, Dean of Columbia SIPA. This conversation set the stage for an afternoon of discussions around cyber security.

The Nuclear Analogy

Janow opened the conversation by highlighting the absence of a clear cyber analogue to mutual assured destruction, and of norms, doctrines, agreed-upon frameworks, and shared understandings of the destructive power represented by cyber conflict. Sanger suggested that members of Congress who grew up during the Cold War are likely to believe that nuclear deterrence is replicable in the cyber realm. But while the questions may be similar for cyber, the answers are different, in part because the weapon is fundamentally different. While nuclear weapons are supremely expensive, cyber weapons are cheap and can be developed with little more than laptops, motivated millennials, and stolen NSA code, which is unfortunately readily available. The U.S. is one of only nine countries in the world with nuclear weapons, but one of 35 that can execute serious, sophisticated cyberattacks.

Cyber deterrence is further complicated by the slowness and difficulty of



attribution; for example, it took until 2019 for the U.S. to indict the leader of the North Korean attack on Sony in 2014. Perhaps more significantly, the U.S. still believes it has a big lead in this realm and is unwilling to sign on to norms that could reduce its flexibility. It may seem unquestionable that a Digital Geneva Convention should rule out attacks on systems relating to electricity distribution, financial data, and elections. However, given its Nitro Zeus project to shut down the electric system in Iran, the CIA might disagree. Should we really ban cyberattacks that could minimize casualties by taking the place of kinetic attacks? Should we outlaw election interference that could foil the rise of dictatorial regimes? Would it be better to shut down communications between China and its troops or nuclear weapon operators, or to allow conflict to erupt in the South China Sea? It's not just the rest of the world that's reluctant to agree to norms, but the U.S. as well.

Cyber Policy in the Obama and Trump Administrations

Comparing the cyber policies of the current and most recent presidents, Sanger characterized the Obama Administration as focused on defense as well as definitions for acts of war, vandalism, and sabotage. With lawyers exerting a strong influence, the Administration was hesitant to engage in offensive operations, such as going through China to attack North Korea, or attacking ISIS operators using German cloud services. Shaped by a (perhaps excessively) large set of individuals, the cyber policy was fundamentally cautious.

The Trump Administration has reduced the number of voices in the conversation. By getting rid of a homeland security advisor experienced with cyber as well as the position of Cyber Security Coordinator, the current Administration has eroded its own expertise. Sanger maintained that cyber defense should be designed by people who break into foreign networks for a living, and that the staff dismantling leaves us in a dangerous place and will be the subject of intense scrutiny after a major cyber event occurs. He saw this winnowing as relating less to cyber security than the desire of then-National Security Advisor John Bolton to limit the number of officials with direct access to the President.

The Trump Administration has also devolved more power to the heads of the NSA and U.S. Cyber Command. In August 2018, Trump signed a secret order allowing Cyber Command to go deep into adversary networks. This has resulted in only one major known operation so far: an attempt to prevent Russian interference in the 2018 midterm elections. With the report still classified, it is unclear whether these efforts were effective. Sanger identified this secrecy as part of a trend of reluctance to reveal cyber capabilities undermining deterrence.

Sanger later returned to Russian election interference, pointing out how “wildly underprepared” the U.S. was in 2016, with the Department of Homeland Security categorizing the power grid, communications grid, Washington Monument, and Jefferson Memorial as critical infrastructure, but not the election system. It was a failure to consider where the most critical data was stored and what could happen to it. Sanger asked, “Do I blame the Russians?...What I really blame is us, for not thinking broadly enough. And the question I keep asking, inside The New York Times and outside, is, why would we ever think the Russians would come back and play the same playbook in 2020? When they come back, it's going to be with something different, or it's going to be the Chinese, or the Iranians, or some other set of players.”

Identifying Acts of War in the Cyber Realm

Sanger broke cyberattacks down into four types:

1. Surveillance, an extension of the established practices of tapping calls and opening mail.
2. Data manipulation, which could involve changing financial or blood type records. With Stuxnet, the U.S. manipulated the input data to Iranian centrifuges, forcing them to slow down or speed up.
3. Using computer controls to make real-world systems go awry. Sanger cited the example of Boeing airplanes crashing because of a misread between two sensors feeding into an automatic flight controller. While these were accidental, it's easy to imagine a malicious actor triggering such a misread.
4. Influence operations, which aren't fundamentally about cyber, but instead using the Internet to quickly and widely disseminate propaganda.

Alluding to Sanger's stated position that the cyber defense doctrine and public dialogue are underdeveloped, Battelle wondered if a major event could trigger the necessary conversations. Sanger suggested that an electrical or Internet outage might be sufficient. He referred to the argument of former White House Chief of Staff Leon Panetta that more funding is needed to prevent a cyber Pearl Harbor. However, Sanger saw such an escalation as unlikely to occur, since it has the potential to call down the sort of military reprisal that states use cyber to avoid. Above all, "cyber Pearl Harbor" sounds like something members of Congress would prefer not to be blamed for and so has the potential to spur action.

Sanger considered whether the U.S. may already have experienced cyber acts of war. If, rather than bringing down 70% of Sony's computing systems firmwide, North Korea had physically attacked a Sony property in Hollywood, the U.S. would likely have attacked Pyongyang. But in the absence of visible smoke or an immediately obvious culprit, it did not retaliate.

Retaliating in the cyber realm might not even be effective against states like North Korea with little online infrastructure to disrupt.


Sanger emphasized that for deterrence to work, "People have to feel that they're paying a price if they're going to do a cyberattack."

North Korea received a few sanctions, but probably didn't feel them too acutely, given all its other sanctions, and Russia paid no price. In this context, Sanger could see the

logic of Israel's May 2019 kinetic response to a Hamas cyberattack, bombing the building allegedly housing



David Sanger



the hackers: Israel was attempting to rattle adversaries who expected retaliation only within the cyber realm. However, he also wondered whether Israel had crossed a Rubicon, since there's no clear precedent for this kind of response. It suggests a future of unpredictable responses and rapid escalation.

China and the New Berlin Wall

Battelle pointed out that China, with its potential dominance of AI, perfection of a surveillance society, size, abundance of data, and government support for companies, has arguably become more of a threat than any other country. It is certainly a major player in the geopolitical standoff over 5G. Sanger explained that 5G involves rewiring the Internet for the Internet of Things, making it a much more significant change than 3G or 4G. At the end of 2018, there were around 14 billion Internet of Things devices in the world; this number will likely climb to 20 billion by the end of 2020. The 5G network, largely software with a switch underneath, will be updated as often as linked devices are, making it nearly impossible to examine every update for backdoors China may have built in. Users don't do code analysis every time we update our phones—we simply trust that the updates are safe.

As 5G spreads around the world, countries are essentially having to declare allegiance with either the U.S. or China. Secretary of State Mike Pompeo has threatened that the U.S. will no longer share intelligence with countries that sign on with Chinese 5G licensor Huawei. Sanger predicted that within two years, "5G could well end up being the new Berlin Wall," forcing each country to side with China and Russia, using the Internet to control populations, side with the free West, or strike a precarious balance and attempt to live on both sides. The U.S. will have to decide whether to freeze out all countries on the authoritarian side or live with a dirty, mixed network.

Reluctance to sign on with Huawei could drive the business of competitors such as Ericsson, Nokia, and Samsung, or catalyze a crash program to get more U.S. companies into 5G. But no matter the service, 5G will be rolled out within a year in major American cities, and Huawei will have forty to sixty percent of the world market. The U.S. will be forced to deal with countries that rely on Huawei switches, which China could shut off in a conflict.

SESSION FIVE

Global Governance and Cyber Conflict

Laura DeNardis

Professor, American University

Angela McKay

Senior Director, Cybersecurity Policy and Strategy, Microsoft

Greg Rattray

former Director, Global Cyber Partnerships & Government Strategy, JPMorgan Chase

Jason Healey

Senior Research Scholar, Columbia SIPA (moderator)




Background

Conflict in cyberspace—primarily but not exclusively between states—seems increasingly uncontrollable. The UN Group of Government Experts made progress for several years, but as their conclusions have partially unraveled, they have split into two separate and competing efforts. Many Western states believe international law applies but the devil is in the details, while other states do not concede even this point.

The U.S. government asserts that it is one of few nations respecting norms of behavior and therefore must change strategies to make it easier to, in the words of General Paul Nakasone of U.S. Cyber Command, “take this fight to the enemy, just as we do in other aspects of conflict.” National Security Advisor John Bolton’s threat was clear: “our hands are not tied” as they were in previous administrations. Recent attacks like North Korea’s WannaCry and Russia’s NotPetya were indeed reckless and dangerous, causing global disruption.

But not all stakeholders agree that the U.S. has been respecting norms, or that a more “forward defense” will be stabilizing. The U.S. wants a secure cyberspace, but not one so secure that it cannot conduct significant espionage operations (as revealed by Edward Snowden) and cyber-enabled



covert action (such as Stuxnet against Iranian nuclear enrichment), and at least retain the option of strategic and battlefield cyber offensive operations (such as the Nitro Zeus operation planned against Iran).

Meanwhile, the underlying technologies continues to change in fundamental ways, especially the growing Internet of Things, which will drastically increase societal and economic dependence on insecure networks and systems. Cyberattacks that in the past might have been ignored or worked around may soon become existential.

The private sector, which both creates and uses these technologies to deliver national critical functions, can be caught in the middle but is an essential partner for global governance. Its priorities, such as resilience, may be useful starting points for global agreement.

Panelists

In the fifth panel of the Forum, cybersecurity and strategy experts from both academia and industry surveyed the forms that Internet governance has taken so far, highlighted tools and techniques that could and should be used more effectively, and called attention to new and understudied threats.

Cyber Governance

Rattray opened the discussion with a survey of historical and current responses to the risks an increasingly digital society poses. Internet governance has come in a variety of modes for different goals and problems, with varying levels of efficacy. With the Internet Corporation for Assigned Names and Numbers, for example, shareholders govern connectivity through the directory of domain names. Governments have been addressing cybersecurity and stability since at least 1998, when Russia made a proposal for arms control in cyberspace.

Russia's early efforts demonstrate how the principles and priorities of each country shape its approach to these issues. DeNardis suggested that Russia was perhaps ready to engage with the issue of Internet content relatively early because authoritarian governments are more comfortable cutting off the flow of information. The U.S. abides by Section 230 of the Communications Decency Act, shielding information intermediary platforms from liability for user content, out of First Amendment concerns. DeNardis viewed recent proposals that might chip away at free speech norms in the U.S. with concern.

In the past decade, the UN has led the dialogue about how to govern the security of cyberspace. Healey noted that this has become a rich space, with a proliferation of working groups and accords led by states, multilateral institutions, and participants from the private sector.

Norms, Deterrence, and Accountability

While there has been progress in this space, it remains to be seen how we can leverage that progress to go beyond norms. McKay recalled that Microsoft testified before the Department of Homeland Security in 2008 about the escalating environment of cyberattacks and the importance of creating “rules of the road” and mechanisms for accountability. Over a decade later, those rules are still not widely agreed upon.

Ratray regarded the UN General Assembly's 2015 cyber principles as the type of normative basis we need. These principles included the idea that critical infrastructures are off-limits from attack during peacetime, highlighting a weakness in this type of governance: states may choose to disregard it. The necessary next step is to develop mechanisms to enforce accountability when norms are transgressed. The private sector may be more capable of creating accountability and should take part in the process of structuring agreements. Much more needs to be done to catch normative and enforcement structures up with rapid technological advances.

McKay highlighted the shortcomings of current deterrence mechanisms. We are in a scary moment in the trajectory of cyberattacks, with too few actors and acts deterred. Tradecraft was not used well enough in response to attacks like WannaCry and NotPetya, with broad societal impact. We must ensure that those who commit significant transgressions face significant consequences.

Under the Trump Administration, there has been a shift towards more calling out of nations that violate norms, with mixed results. Ratray felt that we should get into the habit of doing more to identify transgressions and achieve accountability. But in the current geopolitical environment, “naming and shaming” is intertwined with a host of complex issues. Global companies, less enmeshed in geopolitics than governments, may be able to leverage this tool more effectively to protect the technical and economic functionality of systems.



McKay saw recent cases as falling short of effective “naming and shaming.” They have consisted mostly of naming, with insufficient efforts to make consequences visible. As a result, the impacts of the attacks—why they matter, how they connect to the rules of the road—have remained opaque. The U.S. has made some progress through the Cyber Deterrence Initiative and collaborative efforts with partner governments to create escalation and de-escalation mechanisms to ensure that consequences for this type of behavior are proportional. Of course, as Healey pointed out, EU members may argue that the U.S. itself has faced insufficient consequences for spying on them.

In response to an audience question, Ratray discussed the way in which an overbroad application of the term “attack” to any malicious action on the Internet is complicating the work of deterrence. “Attack” can mean Russians using a virus on Ukraine with global effects, or actions targeting a single individual’s computer. It’s difficult to determine which “attacks” require a response. Espionage is another complicating factor—states have typically agreed that espionage is permissible. Yet computer intrusions are illegal under domestic law. Clarity and governance parameters around permissible behavior are essential for ensuring certain crucial levels of activity, such as protecting critical economic functions and infrastructure that governments can keep off



limits in the broader agreements under discussion.

Healey referred to the work of Adam Segal of the Council on Foreign Relations illuminating the U.S.-China deterrence dynamic. China believes that the U.S. is much better at attribution within both the government and private intelligence communities. The ability of only one side to catch the other cheating undermines willingness to enter into agreements on norms. This potential attribution mismatch makes deterrence more complicated than it was in the Cold War, when both sides could use satellites to monitor each other's missile fields.

Expanding Stakeholders

The panel advocated for an expanded understanding of the stakeholders in Internet governance. Many different players have roles in constructing and architecting for stability. McKay highlighted the 2018 Paris Call as a success in drawing more stakeholders to the table, with over 60 governments, 400 institutions, and 200 global companies signing up to a series of cyber commitments. This kind of support from states, companies, and civil society strengthens the norms developed through governmental processes. In the case of a working group sponsored by a particular state, the identity of the state matters, but not as much as the objective and composition of the stakeholders. Open-ended working groups allow more people to contribute, consistent with the open environment of the Internet.

McKay called for an increased role and sense of responsibility for industry. Companies should collaborate, pledge not to take offensive actions, and help customers defend themselves. The general public is a crucial piece of this puzzle. Too many people don't understand or feel the impact of cyberattacks. One of the few upsides to emerge from election interference has been a more informed public. For people to address a problem, they need to understand it. This was the logic behind Microsoft's 2018 call for a Digital Geneva Convention—the framing was an effective way to democratize the idea that we need legally binding rules of the road for cyberspace and the power to create real accountability for transgressions. Microsoft has also launched an initiative called Digital Peace Now to educate and empower the public.

Public officials, such as policymakers and operational leaders, must also work to foster public understanding. Changing the way cyberattacks are reported and discussed could help the public understand the stakes. The discussion tends to focus on how many computers were hit, which has little resonance with the public. Framing these attacks in more relatable terms—the people who had their surgeries postponed and lives disrupted when the NHS was attacked, the Ukrainian small businesses forced to close after losing their online presence—connects the cyber realm to values and daily life and compels action.

Rattray echoed this call for public engagement and responsibility in response to a question from the audience. He pointed out that individuals have been “hackable entities,” subject to monitoring by criminals and law enforcement, essentially since the advent of telecommunications. But while individual hackability may not be new, it certainly reiterates the importance of responsibility and empowerment. Getting people to pay attention

to individual responsibility becomes even more pressing as the Internet of Things embeds itself in the home.

DeNardis echoed the importance of user awareness and responsibility as technology becomes more complicated, and even those who eschew screens may be unwittingly swept up in the screens of others. With individuals unable to consent to being on those screens, notice and choice are erased. For DeNardis, addressing this requires an emphasis not on civil liberties or human rights, but the collective good.


New Vulnerabilities

DeNardis argued that we are entering Cyber Conflict 2.0, which will play out not exclusively in the cyber world, but the cyber-physical. The potential for this kind of attack dates back over a decade, when the wireless capability of Dick Cheney's cardiac monitor was disabled to prevent assassination via the Internet. More recent examples include Russian cyberattacks on the Ukrainian power system. Despite its extraordinarily high stakes, including privacy and human safety, the Internet of Things is incredibly insecure. Policy and scholarship on the challenges of the cyber-physical world lag behind the technology. Corporate stakeholders are no longer limited to traditional tech companies, but include all companies that collect and make use of data. The distinction between the virtual and physical worlds has disappeared, significantly complicating Internet governance.



To demonstrate the urgent need for change in this space, DeNardis raised a hypothetical question: what if rather than exploiting social media or releasing hacked emails, Russian interference in the 2016 election had targeted the Internet of Things? Malicious actors have demonstrated their ability to disrupt the power grid, interfere with home systems including alarms, and take down public transportation. If such tactics were employed in a targeted way to disable polling places or suppress voter turnout in swing districts, the co-opting of infrastructure would become a proxy for political power. The early Internet was largely for computation. It then evolved into a tool for communication. We must now assess what governance and conflict mean as the Internet becomes a control network.

Healey raised one possible cause for optimism: the suggestion from Jack Snyder, a professor in Columbia's Data Science Institute, that while espionage and cyber engagement will continue, there may be fewer "big swings" that could trigger inadvertent escalations from the cyber realm to the kinetic, potentially resulting in death, destruction, or destabilization of the Internet itself. McKay articulated another aspiration relating to the division between cyber and kinetic conflict: the establishment of a stable ecosystem in which cyber is recognized as a valid tool to be used when armed conflict would be ineffective or disproportionate.



However, the overall consensus was one of great concern. Healey pointed out that while things seemed bad a decade ago, they have grown worse with each year that passes. If cyberattacks begin leading to real-world death and destruction, we may someday look back at even this moment with nostalgia.

For McKay, progress has been insufficient relative to the evolving risk environment. With increasing risks including the number of state and non-state actors with cyber capabilities, the proliferation of tools, and the dramatic increase in the number of sophisticated attacks, the need for progress in this space is urgent. The problems of cybersecurity will only grow more intractable when attacks are AI-enabled or autonomous.

DeNardis argued that we have made a decision as a society to have weak cybersecurity. Weak cybersecurity benefits governments that want to conduct surveillance and foreign espionage as well as companies that want to get goods to market quickly. We must take steps such as banning systems with zero upgradability or weak or default passwords. Only by committing to stronger cybersecurity can we improve the situation.

CYBERSECURITY FIRESIDE CHAT

Lt. Gen. John D. Bansemer (Ret.)

in conversation with:

Greg Rattray

*former Director, Global Cyber Partnerships
& Government Strategy, JPMorgan Chase*




Greg Rattray and Lt. Gen. John D. Bansemer (Ret.)

The fireside chat featured keynote speaker Lt. Gen. John D. Bansemer (Ret.) in conversation with Greg Rattray, Director of Global Cyber Partnerships and Government Strategy at JPMorgan Chase. Drawing on their years of service in national security, Bansemer and Rattray evaluated key opportunities and challenges in the rapidly evolving technological landscape.

Government, Industry, and National Cybersecurity

As Bansemer noted, the government is better suited to reaching some goals than others. Rattray agreed that many major cybersecurity problems elude policy solutions, due in part to the weaknesses inherent to global governance via norms. While norms might provide guidance on which behaviors can be expected and what nations should do, the lack of effective mechanisms for accountability and enforcement has undermined implementation.

Further complicating governance, cyber operations and expertise are located largely in the private sector. Cyberattacks and coercive behaviors between nations play out in private systems, placing corporate security and operations centers on the frontlines and making strong partnerships between government and industry crucial. With the recognition that



collaboration is essential and that specific risk identification, intelligence support, information sharing, and planned contingency responses are needed, dialogue has developed between the private sector and key agencies like the departments of Homeland Security, Energy, and the Treasury. But progress is limited because too little private sector expertise is embedded within government authorities. U.S. policies as well as corporate concerns about the effect of government ties on brand identity have further limited communication between the sectors.

New Challenges

The pace of change poses significant challenges to both the private and public sectors. Rattray cited the Department of Defense's 1985 "Orange Book," outlining the standards, mechanisms, and controls necessary for cybersecurity, with recommendations for the private sector for building trusted capabilities into products. Companies that do not routinely build in such capabilities are unlikely to start now, having little incentive to undertake lengthy security evaluations and lose their race to the market.

The lack of progress in cybersecurity over the past decade is of particular concern as we approach a new threshold with artificial intelligence. As Bansemer observed, AI is inextricably tied to cybersecurity yet also comes with a distinct set of challenges. Among these are significant societal changes that will impact national security. The research of the OECD on the future of work suggests that job displacement will leave large swaths of the population behind. Bansemer wondered where funding will come from to retrain the work force, and suggested that we will need to either bake a bigger pie or cut the pie in different ways. Since large disaffected populations can create significant challenges for governments and overall systemic instability, policy establishing and funding job retraining will be needed in both democratic and non-democratic governments.

Considering current cybersecurity investment, Bansemer expressed optimism about the extent to which the government can secure its own networks. However, new risks creep in around critical infrastructure. To show how this can go beyond cybersecurity, Bansemer cited an Israeli study in which researchers added or removed cancer indicators from CT scans, fooling many radiologists. The opportunity for tampering arose because the original images lacked digital signatures and were sent across unsecured networks. Similar problems could arise if AI capability is developed within a vacuum, without regard to the mechanisms needed to secure the overall system. Meaningful progress will require teams that can build AI functionality while also recognizing the cyber mechanisms necessary to protect the system.

Multidisciplinary Solutions

With economic incentives continuing to result in systems that are less than fully securable, Rattray doubted that problems in cybersecurity will be solved through purely technical means. Nor will governance alone solve these problems, though mandating prudent out-of-the-box default settings on Internet of Things devices could reduce reliance on individual users for security configurations. Bansemer expressed support for multidisciplinary solutions, suggesting that the field of behavioral economics may shed light on how the government can "nudge" good behavior and positive societal outcomes. He saw a further role for academia



in researching vulnerabilities and the steps necessary to secure systems, and in formulating policies to address AI's potential displacement of much of the global population. The private sector has a crucial role of its own to play in developing effective cybersecurity mechanisms and leveraging AI for good.

SESSION SIX

Financial Stability in an Era of Growing Cyber Risk

Jason Healey

Senior Research Scholar, Columbia SIPA

Patricia Mosser

Senior Research Scholar, Columbia SIPA

Tom Wipf

*Vice Chairman of Institutional Securities,
Morgan Stanley*

Katheryn Rosen

*Senior Research Scholar, Columbia SIPA
(moderator)*



Background

Since the financial crisis a decade ago, government authorities and the financial sector have been working to improve overall resilience and financial stability. Parallel to these efforts, governments and industry have been grappling with more frequent and sophisticated cyberattacks and an ever-growing reliance on technology. Initiatives such as SIPA's project on Cyber Risk to Financial Stability (CRFS) examine the gaps in our understanding of the way these realms of risk intersect and promote efforts to build resilience in the financial system.

The financial sector is at the forefront of cybersecurity and industry-wide information sharing and collaboration. Over the last few years, institutions have been built to increase resilience within the financial sector, while research and regulatory efforts have begun to acknowledge and analyze cyber risks to financial stability. However, there is more work to be done. For example, there remains a lack of globally coordinated policies and regulations and little understanding of the technology mapping of financial system processes and the way new technologies will impact markets and systems.

Panelists

In the sixth session of the Forum, a panel of experts from academia and industry considered efforts to date in financial stability and cyber risk, key priorities for government, industry, and academia, potential challenges ahead, and prescriptions to increase resilience.

Managing Risk in the Financial System


Mosser opened the panel with an overview of financial stability. The financial system is hit by thousands of shocks every day. In contrast with cybersecurity, financial stability is not about stopping or identifying shocks. It instead involves monitoring, measuring, and creating institutions, markets, infrastructures, and regulatory structures that shore up the resilience of the entire system no matter what hits it. The approach of those that monitor and attempt to reinforce financial stability, such as regulators, central banks, the International Monetary Fund, and the Financial Stability Board, begins with the recognition that the system is complex and adaptive.

Mosser went on to explain that the financial system is largely robust but occasionally suffers catastrophic crises. While these, fortunately, are rare, it is nearly impossible to predict when they will occur and what shock will trigger them. Policy institutions focus instead on measuring the amplifiers and feedback mechanisms that make the system fragile in the first place, particularly leverage and maturity transformation, which involves financing long-term illiquid assets through short-term liquid borrowing. These functions are common to all financial systems. Because financial risk is



procyclical and endogenous, rising asset prices create a feedback loop with increasing leverage and maturity transformation, resulting in a bubble. This feedback loop also works in reverse, resulting in bank runs and crises. To monitor these cycles, regulators measure leverage levels, price and risk procyclicality, and maturity transformation. The system is complex, interconnected, and opaque. Idiosyncratic shocks to individual firms are not in fact idiosyncratic—the way one bank reacts to a shock instead affects the entire system. Cyber risk mitigation focuses primarily on preventing and containing shock, largely at the level of individual firms, and pays little attention to what business and financial reactions will be to an attack. However, it is those business and financial reactions that can feed into contagion and feedback mechanisms.

To illustrate potential fragilities in financial systems and the dangers of failing to understand how financial channels and feedback mechanisms transmit cyberattacks, Mosser provided the example of the tri-party repo market. This market, widely used by banks and securities dealers, is key for funding and financing securities.



As the financial crisis demonstrated, it is also quite fragile. This is due, in part, to its highly concentrated infrastructure, with a single provider essentially supporting the entire market. Further, it is highly levered and effects massive maturity transformation, sometimes from overnight borrowing to 30-year Treasuries. Since the crisis, massive regulatory and private sector efforts have sought to address the vulnerabilities of the tri-party repo market to financial risk, but some remain. At this point, it is largely unknown how vulnerable this market may be to cyber risk. Rosen made the ominous observation that the many white papers addressing the market's vulnerability to financial risk may even have opened it to cyber risk by providing potential adversaries with a detailed roadmap to the flow of funds.


Comparing Cyber Risk and Financial Risk

Healey described both the financial sector and cyberspace as complex and opaque. The difficulties of understanding how each system works on its own are only amplified when examining the two together. A fundamental difference between the two is the financial sector's maturity in the process of recognizing its own fragility. Healey speculated that there would be much denial if he raised the possibility of a widespread cloud failure or a crucial IT company having a Lehman movement. To achieve a comparable level of self-knowledge, cyber requires much more study and improved metrics. Further, it lacks the governance and response mechanisms of the financial realm. The crisis triggered swift national and supranational responses from central banks, the International Monetary Fund, the Bank of International Settlement, and the G8. The cyber realm simply has not developed global governance or crisis management structures. Who in cyber could call together heads of state and CEOs to respond to a large-scale cyber crisis in the way the Federal Reserve did for the financial crisis?

For Healey, intent is foremost among the dissimilarities between the two realms. In finance, bad results can arise when self-interested behavior aligns, but there tends to be a powerful alignment of interests in the desire to avoid a financial crisis. In cyber, rather than misaligned incentives, there are adversaries with the strategic goal of planned, repeated attacks on systems and processes they understand well enough to target at peak vulnerability. The primary failure mode also differs between these two spaces. For finance, it's contagion, a term borrowed from public health to describe the way a failure can spread. For cyber, the greater risk is common mode failure—a successful attack on Microsoft or Google could affect everyone who uses their systems.

Mosser pointed to another contrast: the long history of international cooperation and standard setting on financial matters. Groups like the Basel Committee, the International Organization of Securities Commissions, and the Committee on Payments and Market Infrastructures (formerly the Committee on Payments and Settlement Systems) work out a consensus on minimum standards, then convince national regulators to put them into law. Cyber lacks this historical roadmap for successful cooperation. Cyber also has a national security intent aspect that is absent from other conversations about international standard setting for the financial system. This makes the establishment of hard agreements much more difficult.

Despite the many differences between these realms and the frailties inherent to each, Healey emphasized that



there is also resilience, extraordinary efforts from determined problem solvers, and strength from leaders accustomed to making incredibly tough calls in times of crisis. We can strengthen this resilience through exercises that develop agility, creating “muscle memory” to draw on in a crisis. In response to an audience member’s question about chaos engineering, Healey praised Netflix’s efforts to ensure seamless service even in an outage by running self-attacks. He suggested that the Department of Defense ought to employ this strategy to strengthen the resilience of its own networks.

Cyber Risk to Financial Stability

A growing body of studies is examining the interrelation between cyber and financial risk. Mosser highlighted the work of Stanford’s Darrel Duffie on liquidity runs in response to cyberattacks. MIT has made inroads on understanding risk management and measurement metrics. The Bank of England has released principles for how to think about regulating cyber risk.

Joining these efforts, the SIPA CRFS examines the transmission of cyberattacks across systems, not just through technology but also financial channels and feedback mechanisms. Through an extensive literature review, numerous workshops, and a flagship conference gathering both cyber and financial practitioners from government, industry, and the academy, the CRFS has worked to develop a framework for assessing the linkages between cyber risk and financial stability. The CRFS analytical framework begins with two questions: i) how a particular cyber risk may initiate an episode of financial instability, and ii) how a financial vulnerability in a particular part of the system could be exploited by cyber adversaries. These questions are critical to understanding cyber risk transmission channels. This systemic-level of analysis, inclusive of the amplifiers and dampeners of such risks, will help shore up financial and cyber resilience beyond the enterprise, to the financial system.

For Healey, one of the strengths of this framework is allowing us to approach the problem from either direction. We might examine how a cyber incident could affect a particular element of a well-understood market. Or we could begin with a hypothetical cyber incident and extrapolate how it might affect transmission mechanisms. For example, imagining a successful cyberattack on Microsoft illuminates the absence of substitutability, since it’s so widely relied upon. We can then evaluate how such an attack might impact financial markets.

The Role of Industry

Wipf provided a perspective on how the financial sector can improve its understanding of and response to new risks. Gaps must be closed at both the level of industry and that of the firm. Across firms, different teams deal with problems like denial of access, financial stress, and cyber events. Things that impact operations also impact asset prices, market access, and the ability to trade. Making these connections clear, along with testing and tabletops, can lead to a closer alignment between the behavior recommended by playbooks and the actions of individuals in times of stress. Individuals on the trading side are too infrequently in the same room with those who deal with cyber problems. Front-to-back connections within a firm between those who are

impacted and those who can see the impact may sound like straightforward good housekeeping, but in many large organizations, the gap remains. Pulling together more quickly and effectively will lead to more efficient resolutions.

For Wipf, once interconnectivity becomes clearer within the firm, the next step is to expand it out to the sector more broadly. Industry-wide exercises such as the Financial Services Roundtable have driven cooperative problem solving. In parallel with recent work on clearing and settlement by the Treasury Market Practices Group of the Federal Reserve, the Financial Systemic Analysis and Resilience Center (FSARC) ran an exercise focused on cyber outages in the Treasury market. The intersection of Fed maps and subject matter expertise from FSARC resulted in new insights about market utilities and access and how infra-

structure connects to trading. To make competitors more open to this kind of information sharing and improve resilience, Wipf proposed that the industry adopt a team sport mentality.



Tom Wipf

SPEAKER BIOGRAPHIES



Lt. General John D. Bansemer (Ret.)

John Bansemer served in a variety of cyber, space and intelligence positions within the U.S. Air Force before retiring recently as a Lieutenant General. His last role was serving as an Assistant Director for National Intelligence within the Office of the Director of National Intelligence supporting worldwide partner engagement efforts. Previously, he served in various operational and staff positions including on the National Security Council staff and as the director of intelligence at European Command. He continues to research and support studies in cyber and emerging technologies focusing on their national security implications.



John Battelle

Co-Founder and CEO, Recount Media
Senior Research Scholar, Columbia SIPA

John Battelle is co-founder/CEO of Recount Media, a political media platform currently in development, and serves as a Senior Research Scholar and Adjunct Professor at Columbia University/SIPA. Battelle also runs NewCo, an “inside out” conference model and media platform. He also serves as Chair of Sovrn Holdings, a publisher-first programmatic advertising and data platform that proudly serves 100,000+ sites. He has founded or co-founded more than half a dozen companies across media and technology, including Federated Media Publishing, the Web 2 Summit, Standard Media International (SMI), publisher of *The Industry Standard* and *TheStandard.com*, and *Wired* magazine. He is also a director at LiveRamp, a NYSE-listed data services business. In 2005 he authored *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (Penguin/Portfolio), an international bestseller published in more than 25 languages.



Josh Benaloh

Senior Cryptographer
Microsoft Research

Josh Benaloh is Senior Cryptographer at Microsoft Research and an Affiliate Faculty Member of Computer Science and Engineering at the University of Washington. He earned his S.B. degree from the Massachusetts Institute of Technology and M.S., M.Phil., and Ph.D. degrees from Yale University where his 1987 doctoral dissertation “Verifiable Secret-Ballot Elections” introduced the use of homomorphic encryption as a means to allow individual voters to confirm that their votes have been correctly counted. Dr. Benaloh served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network. He has been granted over fifty U.S. patents and has written and spoken extensively on cryptographic primitives and protocols, election technologies, and cryptographic policy. Dr. Benaloh is an author of the influential “Keys Under Doormats” expert report which details the damage that would be created by mandating exceptional government access to encrypted data. He is also an author of the U.S. Vote Foundation report on the viability of end-to-end verifiable Internet voting systems and recently completed service on the National Academies of Science, Engineering, and Medicine Committee on the Future of Voting whose final report “Securing the Vote—Protecting American Democracy” has been cited in numerous articles and deliberations.

**Laura DeNardis**

*Professor, American University
Senior Research Scholar, Columbia SIPA*

Dr. Laura DeNardis is globally recognized as one of the most read scholars in Internet governance. She is a tenured Professor in the School of Communication at American University in Washington, DC, where she serves as Faculty Director of the Internet Governance Lab. In 2018, she was the recipient of American University's highest faculty award, Scholar-Teacher of the Year. Her six books include *The Global War for Internet Governance* (Yale University Press 2014); *Opening Standards: The Global Politics of Interoperability* (MIT Press 2011); *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009); among others. Her new book, *The Internet in Everything: Freedom and Security in a World with No Off Switch*, is forthcoming from Yale University Press. She is an affiliated fellow of the Yale Law School Information Society Project and served as its Executive Director from 2008-2011. Her expertise and scholarship have been featured in *Science Magazine*, *The Economist*, National Public Radio (NPR), *The New York Times*, *Time* magazine, *Christian Science Monitor*, *Slate* magazine, *Reuters*, *Forbes*, *The Atlantic*, and *The Wall Street Journal*, among others. She holds an Engineering Science degree from Dartmouth College, an MEng from Cornell University, a PhD in Science and Technology Studies from Virginia Tech, and was awarded a postdoctoral fellowship from Yale Law School.

**Renee DiResta**

*Mozilla Fellow
Media, Misinformation, and Trust*

Renee DiResta is a Mozilla Fellow in Media, Misinformation, and Trust and a Staff Associate at Columbia University Data Science Institute. Renee investigates the spread of disinformation and malign narratives across social networks, and has advised Congress and the State Department on the topic. She was the lead author on one of the Senate Intelligence Committee-commissioned reports on Russian interference in the 2016 election. Renee is a 2019 Truman National Security Fellow, a 2017 Presidential Leadership Scholar, a Harvard Berkman-Klein affiliate, a Council on Foreign Relations term member, and a Founding Adviser to the Center for Humane Technology. She is an IDEAS contributor for Wired.

**Victoria Espinel**

*President and CEO
BSA | The Software Alliance*

Victoria Espinel is a respected authority on the intersection of technology innovation, global markets and public policy. She leads strategic efforts that help shape the technology landscape in 60 countries through work in BSA's 13 global offices. Espinel also serves as the President of Software.org: the BSA Foundation. Software.org is an independent and nonpartisan international research organization created to help policymakers and the broader public better understand the impact that software has on our lives, our economy, and our society. Espinel served for a decade in the White House, for both Republican and Democratic Administrations as President Obama's advisor on intellectual property and, before that, as the first ever chief US trade negotiator for intellectual property and innovation at USTR. She was also a professor of international trade and intellectual property at the George Mason School of Law.

**Jameel Jaffer**

*Director of the Knight First Amendment Institute,
Columbia University*

Jameel Jaffer directs the Knight First Amendment Institute at Columbia University, whose mandate is to defend the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. Since its establishment three years ago, the Institute has initiated cutting-edge litigation relating to free speech on social media, surveillance, and government secrecy, and it has launched several major research projects—most recently, a project focused on “the technology giants, monopoly power, and public discourse,” which will culminate in a symposium at Columbia University in the fall of 2019. Jaffer previously served as deputy legal director at the ACLU, where he oversaw the organization’s work on free speech, privacy, technology, national security, and international human rights. Jaffer’s recent writing has appeared in *The New York Times*, the *Washington Post*, the *Los Angeles Times*, the *Guardian*, and the *Yale Law Journal Forum*. He is an executive editor of Just Security, a national security blog, and his most recent book, *The Drone Memos*, was published by The New Press in the fall of 2016.

**Ronaldo Lemos**

*Director, Institute for Technology and Society of Rio de Janeiro;
Visiting Professor, Columbia SIPA*

Ronaldo Lemos is an internationally respected Brazilian academic, lawyer and commentator on intellectual property, technology, and culture. Lemos is a co-founder and director of the Institute for Technology & Society of Rio de Janeiro (itsrio.org), and professor at the Rio de Janeiro State University’s law school. He is a board member of various organizations, including the Mozilla Foundation, and Access Now. Lemos was one of the creators of Brazil’s Internet Law (Marco Civil da internet), enacted in April 2014, creating a comprehensive set of rights for the internet in Brazil, including freedom of speech, privacy and net neutrality. Because of its impact in favor of an open and free internet, the Marco Civil has been praised by Tim Berners-Lee “a very good example of how governments can play a positive role in advancing web rights and keeping the web open”. In July 2013, Lemos joined the MIT Media Lab as a visiting scholar. Lemos has received the Prix Ars Electronica Golden Nica in the category of digital communities. He writes weekly to *Folha de São Paulo*, the biggest national newspaper in Brazil, and has contributed to a number of other publications, including *Foreign Affairs*, *Harper’s Bazaar*, and *Bravo!* He also hosts a weekly TV show at Canal Futura, and is a commentator on technology for Globonews.

**Alex Macgillivray**

*Board Member, Data & Society,
and former Deputy CTO of the U.S.*

Alexander Macgillivray is curious about many things including ethics, law, policy, government, decision making, the Internet, algorithms, social justice, access to information, coding, and the intersection of all of those. He was United States Deputy Chief Technology Officer for the last two plus years of the Obama Administration. He was Twitter’s General Counsel, and head of Corporate Development, Public Policy, Communications, and Trust & Safety. Before that he was Deputy General Counsel at Google and created the Product Counsel team. He has served on the board of the Campaign for the Female Education (CAMFED) USA, was one of the early Berkman Klein Center folks, was certified as a First Grade Teacher by the State of New Jersey, and studied Reasoning & Decision Making as an undergraduate. These days he is doing a bunch of coding, writing, and short burst projects with organizations thinking about what they should be doing next. He is also proud to be a board member at Data & Society and advisor to the Mozilla Tech Policy Fellows.



Angela McKay

*Senior Director, Cybersecurity Policy & Strategy,
Microsoft*

Angela McKay is Senior Director of Cybersecurity Policy and Strategy within Customer Security and Trust at Microsoft. She leads Microsoft's public policy work on cybersecurity and cloud security, and helps drive the company's efforts to ensure a peaceful and stable cyberspace. Her team includes professionals working on these topics across Africa, Asia, Europe, Latin America and the US. McKay serves as Secretary for the Coalition to Reduce Cyber Risk, on the Board of Councilors for the East West Institute, and as Microsoft's Point of Contact for the President's National Security Telecommunications Advisory Committee. Before joining Microsoft in 2008, she worked at Booz Allen Hamilton and BellSouth Telecommunications. McKay holds a bachelor's in industrial and systems engineering from the Georgia Tech.



Patricia Mosser

*Senior Research Scholar,
Columbia SIPA*

Patricia C. Mosser is Director of the MPA Program in Economic Policy Management at Columbia University's School of International and Public Affairs and leads the school's Initiative on Central Banking and Financial Policy. Previously, Mosser was head of the Research and Analysis Center at the Office of Financial Research, U.S. Treasury Department. Mosser spent over 20 years at the Federal Reserve Bank of New York where she was a senior manager at the Fed's open market desk overseeing market analysis, monetary policy implementation including many crisis-related facilities, foreign exchange operations, and analysis of financial stability and reform. She previously served as an economist and manager in the New York Fed Research Department and as an assistant professor in the Economics Department at Columbia. Mosser has written on financial stability and monetary policy topics including financial reform, crisis policy tools, and the monetary transmission mechanism. She serves as a consultant to the Bank of England and was previously a member of the Deputies Committee of the Financial Stability Oversight Council (FSOC), the Board of the American Economic Association's Committee on the Status of Women in the Economics Profession (CSWEP) and numerous international central banking and financial policy committees. She received a BA from Wellesley College, an MSc with distinction from the LSE, and a PhD in economics from MIT.



Eli Noam

*Paul Garrett Professor of Public Policy and Business Responsibility Economics, Columbia Business School;
Director of the Columbia Institute for Tele-Information, Columbia University*

Eli Noam is Professor of Economics and Finance at the Columbia Business School since 1976, and its Garrett Professor of Public Policy and Business Responsibility. He is the Director of the Columbia Institute for Tele-Information, a research center focusing on management and policy issues in communications, internet, and media. Noam has published 30 books and over 300 articles. Recent books and projects include: *Who Owns the World's Media* (Oxford); two textbooks: *Managing Media and Digital Organizations & Media and Digital Management* (Palgrave, forthcoming); and the project: A National Initiative for Next Generation Video. Noam advisory board memberships have included the Federal government's telecommunications network, the Nexus Mundi Foundation (Chairman), the Electronic Privacy Information Center, Oxford Internet Institute, Jones International University, and several committees of the National Research Council. He received the degrees of BA, MA, PhD (Economics) and JD from Harvard University, and honorary doctorates from the University of Munich (2006) and the University of Marseilles Aix-la-Provence (2008).

**Greg Rattray**

*Former Director of Global Cyber Partnerships & Government Strategy
JPMorgan Chase*

Dr. Greg Rattray is Managing Director of Global Cyber Partnerships & Government Strategy at JPMorgan Chase, responsible for JPMorgan Chase's cybersecurity policy development, advocacy and relationships with industry partners, clients, government agencies and global organizations. Dr. Rattray led the establishment of the Financial Systemic Analysis & Resilience Center (FSARC), a private-public strategic initiative to understand and reduce risks to the financial system and enhance the level of operational collaboration. Greg joined JPMC in 2014 as the Global Chief Information Security Officer (CISO). Prior to joining JPMorgan Chase, Dr. Rattray was founding partner and CEO of Delta Risk LLC, a cybersecurity risk management consulting firm that focused on addressing advanced cyber threats. He retired from the U.S. Air Force as a Colonel after twenty three years of service including as Director for Cybersecurity in the White House and commanding the Operations Group of the Air Force Information Warfare Center responsible for cyber operations and defending cyber threats.

**Daniela Rus**

*Director of the Computer Science and AI LAB
Massachusetts Institute of Technology*

Daniela Rus is the Andrew (1956) and Erna Viterbi Professor of Electrical Engineering and Computer Science and Director of the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT. Rus's research interests are in robotics and artificial intelligence. The key focus of her research is to develop the science and engineering of autonomy. Rus is a Class of 2002 MacArthur Fellow, a fellow of ACM, AAAI and IEEE, and a member of the National Academy of Engineering and of the American Academy of Arts and Sciences. She is the recipient of the Engelberger Award for robotics. She earned her PhD in Computer Science from Cornell University.

**Samm Sacks**

Cybersecurity Policy and China Digital Economy Fellow New America

Samm Sacks is a Cybersecurity Policy and China Digital Economy Fellow at New America. Her research focuses on emerging information and communication technology (ICT) policies globally, particularly China. She leads the Charting Chinese Data Governance initiative, which publishes translation and analysis of developments related to data protection, cross border data transfer, and China's data policies in global comparative context. She has worked on China's technology policies for over a decade. Previously, she was Senior Fellow in the Technology Policy Program at Center for Strategic and International Studies (CSIS). At CSIS, she published widely cited reports and commentaries on issues ranging from China's cybersecurity standards to comparison between the EU's GDPR and China's data protection system. Before joining CSIS, Sacks launched the industrial cyber business for Siemens in Asia, focusing on energy sector cybersecurity markets in East Asia. Previously, she led China technology sector analysis at the political risk consultancy Eurasia Group. Prior to this, she worked at Booz Allen Hamilton and Defense Group Inc., where she advised senior U.S. government officials on China's science and technology (S&T) development. She reads and speaks Mandarin and is a frequent contributor to print and TV media, including, the BBC, Bloomberg, CNN, the Financial Times, New York Times, Politico, Reuters, Wall Street Journal, and The Washington Post. Her articles have appeared in the Atlantic and Foreign Affairs, among other outlets. She has testified before Congress three times in the last year on the U.S.-China technology relationship. A former Fulbright scholar in Beijing, Sacks holds an MA from Yale University in international relations and a BA from Brown University in Chinese literature.



David E. Sanger

*National Security Correspondent
The New York Times*

David E. Sanger is a national security correspondent and a senior writer. In a 36-year reporting career for *The New York Times*, he has been on three teams that have won Pulitzer Prizes, most recently in 2017 for international reporting. His newest book, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*, examines the emergence of cyberconflict as the primary way large and small states are competing and undercutting each other, changing the nature of global power. He is also the author of two Times best sellers on foreign policy and national security: *The Inheritance: The World Obama Confronts and the Challenges to American Power*, published in 2009, and *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, published in 2012. For *The Times*, Mr. Sanger has served as Tokyo bureau chief, Washington economic correspondent, White House correspondent during the Clinton and Bush administrations, and chief Washington correspondent. A 1982 graduate of Harvard College, Mr. Sanger was the first senior fellow in The Press and National Security at the Belfer Center for Science and International Affairs at Harvard. With Graham T. Allison Jr., he co-teaches Central Challenges in American National Security, Strategy and the Press at the Kennedy School of Government.



JoAnn C. Stonier

*Chief Data Officer,
MasterCard*

JoAnn Stonier is the Chief Data Officer for Mastercard, where she is responsible for the enterprise data strategy and management, including identifying and mitigating data risks across the company, as well as influencing data-driven products, overseeing data policy and governance. She advises executive management on a broad range of complex data policy and regulatory issues. Prior to her current position, Ms. Stonier established the first Privacy Office for Mastercard in 2008, and developed the organization's Information Governance program beginning in 2013. Prior to joining Mastercard, Ms. Stonier was the Chief Privacy Officer for American Express Company. JoAnn is a recognized data and privacy expert and is sought after for her innovative and practical approach to solving problems in the digital age. In 2018 she assisted in the creation and launch of Tru^{data}, an Irish data trust enterprise, formed to ensure anonymization compliance with the EU-General Data Protection Regulation. She currently serves on their board. In addition to the Tru^{data} board of directors, she currently advises a broad range of industry and policy groups regarding data innovation and privacy including: the United Nations Global Privacy Advisory Group; the World Economic Forum's Data Driven Development Steering Committee; and the Board of Directors of the Information Accountability Foundation.



Kara Swisher

*Technology Business Journalist and Co-Founder
Recode*

Kara Swisher is the co-founder and editor-at-large of Recode, producer and host of the Recode Decode and Pivot podcasts, and co-executive producer of the Code Conference series. She also has a special series on MSNBC called Revolution on the impact of technology on work, society, and more, and is a contributing opinion writer for *The New York Times*. Prior to Recode, Swisher co-produced and co-hosted the *Wall Street Journal's* "D: All Things Digital" conference series (now called the Code conference). She was also the co-executive editors of a tech and media website, AllThingsD.com, founded in 2007. Swisher worked in the *Wall Street Journal's* San Francisco bureau. For many years, she wrote the column "BoomTown," which appeared on the front page of the Marketplace section and online at WSJ. com. Previously, Swisher covered breaking news about the web's major players and Internet policy issues and also wrote feature articles on technology for the paper. She received her undergraduate degree from Georgetown University's School of Foreign Service and her graduate degree at Columbia University's School of Journalism. Swisher is also the author of *aol.com: How Steve Case Beat Bill Gates, Nailed the Netheads and Made Millions in the War for the Web*, published by Times Business Books in July 1998. The sequel, *There Must Be a Pony in Here Somewhere: The AOL Time Warner Debacle and the Quest for a Digital Future*, was published in the fall of 2003 by Crown Business Books.

**Eric Talley***Professor**Columbia Law School*

Eric Talley is the Isidor and Seville Sulzbacher Professor of Law and Co-Director, Millstein Center for Global Markets and Corporate Ownership. He is an expert in the intersection of corporate law, governance, and finance, and he teaches/researches in areas that include corporate law and finance, mergers and acquisitions, quantitative methods, machine learning, contract and commercial law, game theory, and economic analysis of law. He is current Chair of the board of directors of the Society for Empirical Legal Studies (SELS) and was the SELS co-president in 2013–2014. He also serves on the board of directors of the American Law and Economics Association (ALEA). Talley is a frequent commentator in the national media, and he speaks regularly to corporate boards and regulators on issues pertaining to fiduciary duties, governance, and finance.

**Mac Warner***Secretary of State**West Virginia*

WV Secretary of State Mac Warner is a graduate of the United States Military Academy at West Point and the West Virginia University School of Law. He also holds two Masters Degrees in International Law from the University of Virginia. During his 23-year career in the United States Army, Secretary Warner served on four continents, deploying to military hot spots around the world while also serving on the staff at the U.S. Army War College. Prior to being elected West Virginia's 30th Secretary of State, Lt. Colonel Warner served five years with the U.S. State Department in Afghanistan. Since taking his oath of office on January 16, 2017, Secretary Warner has been recognized throughout the country for his innovation in cybersecurity and election preparation. Under his leadership, West Virginia became the first state in the nation to offer a mobile voting application designed specifically for overseas military personnel deployed to remote areas of the world during election time. Since becoming Secretary of State, Secretary Warner has led an effort for West Virginia to secure federal funding to assist counties with more than \$12 million in new voting equipment, state of the art election technology and physical security. In addition to his duties as the state's chief elections officer, Secretary Warner also serves as the state's chief business official. Today there are more than 116,000 entities licensed to do business in the Mountain State.

**Fred Wilson***Partner**Union Square Ventures*

Fred Wilson has been a venture capitalist since 1987. He is a partner at Union Square Ventures and also founded Flatiron Partners. Fred has a Bachelor degree in Mechanical Engineering from MIT and an MBA from The Wharton School of Business at the University of Pennsylvania. Fred is married with three children and lives in New York City. Fred is Chairman of the NYC Department of Education's CS4All Capital Campaign and is co-Chairman of Tech:NYC.

**Tom Wipf**

*Vice Chairman of Institutional Securities and
Chair of Treasury Market Practices Group
Morgan Stanley*

Tom Wipf is Vice Chairman of Institutional Securities. In his role, Tom is responsible for assisting the President of Morgan Stanley with regulatory and other matters. Additionally, Tom leads the firm's Global Business Continuity Management Organization, which is responsible for strategic planning and risk management for potential cyber and physical disruptions. Tom is responsible for the firm's transition efforts to alternative reference rates to replace LIBOR. He is a member of the firm's Securities Operating Committee, Risk Management Committee and Asset/ Liability Management Committee. Prior to being named Vice Chairman, Tom was the Global Head of the Bank Resource Management Division where he was responsible for the firm's secured funding, securities lending, global hedging and collateral management activities. Beginning his career in the industry in 1977, Tom joined Morgan Stanley in 1986 and has been engaged in the Firm's funding, collateral and hedging activities throughout his career at the firm. Based in New York, Tom has also completed multi-year assignments in Morgan Stanley's London and Tokyo offices. In April, 2019, Tom was named Chair of the Alternative Reference Rates Committee (ARRC) by the Federal Reserve Board. The ARRC is a group of private-market participants convened to help ensure a successful transition from USD LIBOR to a more robust reference rate. Tom serves as Chair of the Treasury Market Practices Group. Sponsored by the New York Federal Reserve, this industry group is committed to supporting the integrity and efficiency of the U.S. Treasury and Agency Mortgage Securities Markets. Tom was appointed Chair of the US Commodity Futures trading Commission's Market Risk Advisory Committee (MRAC) Interest Rate Benchmark Reform Subcommittee in October, 2018. Tom serves on the board of directors of International Swaps and Derivatives Association, Inc. (ISDA). Tom was appointed to the Alternative Reference Rate Committee, sponsored by the Board of Governors of the Federal Reserve in 2014. Tom previously served on the Financial Research Advisory Committee to the US Treasury Office of Financial Research from 2012 to 2017.

**Tim Wu**

*Professor of Law, Science, and Technology
Columbia Law School*

Tim Wu is a professor at Columbia Law School, and a contributing opinion writer for *The New York Times*. He is best known for his work on Net Neutrality theory. He is author of the books *The Master Switch*, *The Attention Merchants* and *The Curse of Bigness* along with *Network Neutrality*, *Broadband Discrimination*, and other works. In 2013 he was named one of America's 100 Most Influential Lawyers, and in 2017 he was named to the American Academy of Arts and Sciences.

MODERATOR BIOGRAPHIES



Emily Bell

*Director, Tow Center for Digital Journalism
Columbia Journalism School*

Emily Bell is founding director of the Tow Center for Digital Journalism at Columbia's Graduate School of Journalism and a leading thinker, commentator and strategist on digital journalism. Established in 2010, the Tow Center has rapidly built an international reputation for research into the intersection of technology and journalism. The majority of Bell's professional career was spent at Guardian News and Media in London working as an award winning writer and editor both in print and online. As editor-in-chief across Guardian websites and director of digital content for Guardian News and Media, Bell led the web team in pioneering live blogging, podcasting, multimedia formats, data and social media, making the Guardian an internationally awarded beacon of digital transformation. Emily continues to write a regular column for the Guardian and Columbia Journalism Review, and is a contributor to *The New York Times*, CNN, the BBC, and numerous other outlets. She lives in New York City with her husband and three sons.



Anupam Chander

*Professor, Georgetown University Law Center
Senior Research Scholar, Columbia SIPA*

Anupam Chander is a Professor of Law at Georgetown University Law Center. Much of his scholarship focuses on the global regulation of new technologies. His book, *The Electronic Silk Road* (Yale University Press) seeks to "dismantle the logistical and regulatory barriers . . . to trade while at the same time ensuring that public policy objectives cannot easily be evaded through a simple jurisdictional sleight of hand or keystroke." A graduate of Harvard College and Yale Law School, he clerked for Chief Judge Jon O. Newman of the Second Circuit Court of Appeals and Judge William A. Norris of the Ninth Circuit Court of Appeals. He practiced law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton. He has been a visiting law professor at Yale, the University of Chicago, Stanford, and Cornell. Prior to joining the Georgetown faculty, he was the Director of the California International Law Center and Martin Luther King, Jr. Professor of Law at UC Davis. He is an elected member of the American Law Institute, and has previously served on the Executive Council of the American Society of International Law, where he cofounded the International Law and Technology Interest Group. He serves as a judge of the Penn-Stanford Junior International Faculty Forum. The recipient of Google Research Awards and an Andrew Mellon grant on the topic of surveillance, he has served on ICTSD/World Economic Forum expert groups on the digital economy. An affiliate of Yale's Information Society Project, he serves as a faculty advisor to Georgetown's Institute for Technology Law and Policy.



Avril Haines

Deputy Director, Columbia World Projects

Lecturer in Law, Columbia Law School

Avril Haines is a Deputy Director of Columbia World Projects, a Lecturer in Law at Columbia Law School, and a Senior Fellow at the Johns Hopkins University Applied Physics Laboratory. She was appointed by President Obama to serve as a Member of the National Commission on Military, National, and Public Service, co-chairs the U.S. Holocaust Memorial Museum's Simon Skjodt Center for the Prevention of Genocide's Advisory Group, and serves on a number of boards and advisory groups, including the Nuclear Threat Initiative's Bio Advisory Group, the Board of Trustees for the Vodafone Foundation, and the Refugees International Policy Advisory Council. Prior to joining Columbia University, Avril served as Assistant to the President and Principal Deputy National Security Advisor to President Obama. Before that, she served as the Deputy Director of the Central Intelligence Agency. Avril also held a number of senior legal positions in the government, including Legal Adviser to the National Security Council.



Jason Healey

Senior Research Scholar

Columbia SIPA

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict, competition and cooperation. Prior to this, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a Senior Fellow. His was the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012* and co-authored the book *Cyber Security Policy Guidebook* by Wiley. His ideas on cyber topics have been widely published in over a hundred articles and essays published by the World Economic Forum, Aspen Strategy Group, Atlantic Council, and National Research Council. *A Fierce Domain* was reviewed favorably in the *Economist* and by numerous government leaders, including both the President of Estonia and former head of the CIA and NSA. Jason is also president of the Cyber Conflict Studies Association and previously was adjunct faculty at National Cryptologic School, Georgetown University, and Johns Hopkins School of Advanced International Studies. He is an affiliate at Stanford University's Center for International Security and Arms Control. Jason was one of the pioneers of cyber threat intelligence and has unique experience working issues of cyber conflict and security spanning fifteen years across the public and private sectors.



Merit E. Janow

*Dean, School of International and Public Affairs
Columbia SIPA*

Merit E. Janow is an internationally recognized expert in international trade and investment. She has extensive experience in academia, government and business, with life-long experience in the Asia-Pacific. At Columbia University, Professor Janow became Dean of Columbia University's School of International and Public Affairs (SIPA) in July 2013 after serving as a Professor at SIPA and Columbia Law School. In 2014, Janow created the Tech and Policy Initiative at SIPA to initiate new courses on data science and public policy; new efforts around digital entrepreneurship; the Global Digital Futures Forum; and research initiatives around cybersecurity and the digital economy. She has written three books and numerous articles and frequently speaks before business, policy and academic audiences around the world. She served for four years as one of the seven Members of the World Trade Organization's (WTO) Appellate Body. From 1997 to 2000, she served as the Executive Director of the first international antitrust advisory committee to the Attorney General and the Assistant Attorney General for Antitrust, US Department of Justice. Prior to joining Columbia's faculty, Professor Janow was Deputy Assistant U.S. Trade Representative for Japan and China (1989-93). She was responsible for developing, coordinating and implementing U.S. trade policies and negotiating strategies towards Japan and China. Professor Janow negotiated more than a dozen trade agreements with Japan and China. Early in her career, Professor Janow was a corporate lawyer specializing in cross-border mergers and acquisitions with Skadden, Arps, Slate, Meagher & Flom in New York. She currently serves on the boards of several tech and finance companies and non-profit organizations.



Katheryn Rosen

Senior Research Scholar Columbia SIPA

Katheryn Rosen is an Adjunct Professor at Columbia University's School of International Public Affairs focusing on cybersecurity and a non-Resident Senior Fellow at the Atlantic Council-Brent Scowcroft Center on International Security's Cyber Statecraft Initiative. Over a 25 year career, Katheryn has been active in both the public and private sectors. She served at the U.S. Department of Treasury as Deputy Assistant Secretary for Financial Institutions Policy and Senior Advisor to the Assistant Secretary of Financial Institutions. On Capitol Hill, she served as Senior Policy Advisor to House Financial Services Chairman Barney Frank, working primarily on the Dodd-Frank Act and housing finance reform. Prior to her public service, Katheryn, a Managing Director, spent 14 years at JPMorgan's Investment Bank. She led the Government Institutions Group where she was responsible for delivering the Firm's full range of services and products to Government-Sponsored Enterprises (GSEs), US-based multilateral-lending institutions, and the US government. Most recently at BlackRock, Katheryn was a senior leader of the Financial Markets Advisory team where she focused on the impact of regulation, policy, and official sector actions on clients' businesses across banks, GSEs, central counterparties, and official institutions.

**Jeanette Wing**

*Avanessians Director, Data Science Institute and
Professor of Computer Science, Columbia University*

Jeannette M. Wing is Avanessians Director of the Data Science Institute and Professor of Computer Science at Columbia University. From 2013 to 2017, she was a Corporate Vice President of Microsoft Research. She is Adjunct Professor of Computer Science at Carnegie Mellon where she twice served as the Head of the Computer Science Department and had been on the faculty since 1985. From 2007-2010 she was the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation. She received her SB, SM, and PhD degrees in Computer Science, all from the Massachusetts Institute of Technology. Professor Wing's general research interests are in the areas of trustworthy computing, specification and verification, concurrent and distributed systems, programming languages, and software engineering. Her current interests are in the foundations of security and privacy, with a new focus on trustworthy AI. She was or is on the editorial board of twelve journals, including the Journal of the ACM and Communications of the ACM. She is currently a member of: the National Library of Medicine Blue Ribbon Panel; the Science, Engineering, and Technology Advisory Committee for the American Academy for Arts and Sciences; the Board of Trustees for the Institute of Pure and Applied Mathematics; the Advisory Board for the Association for Women in Mathematics; and the Alibaba DAMO Technical Advisory Board.



 COLUMBIA | SIPA
Technology and Policy Initiative