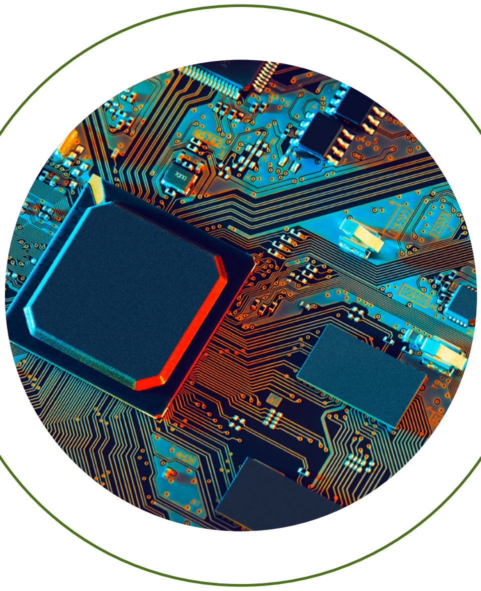
November 2020

#Tech2021



Ideas for Digital Democracy

Edited by Karen Kornbluh and Sam duPont

With Forewords by Rep. Will Hurd and Christopher Schroeder

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

November 2020

Table of Contents

November 2020

FOREWORD

WILL HURD

A critical factor in the United States' economic and military success has been the achievement of global leadership in advanced technology; however, the next administration will inherit the country's most tenuous global position in this area since the Second World War. In today's Fourth Industrial Revolution, technological change over the next 30 years will make the last 30 years look insignificant. The next administration will also deal with a dramatically shifting global landscape influenced by the long-term effects of the coronavirus pandemic and a Chinese government that is trying to rapidly erode U.S. technological advantages through legal and illegal means. Winning this generation-defining struggle for global leadership in advanced technology will not just affect the U.S. economy but will also shape the rest of the century for the entire world. The next administration must have a comprehensive technology agenda to spur innovation in the United States, leverage innovative technologies within government to better serve citizens, mitigate the challenges posed by technological disruption, and work with allies to ensure our democratic values drive development of these new tools.

Though artificial intelligence (AI) is just one of many critical emerging technologies, the blueprint for achieving global leadership in AI can be a useful guide for how the next administration could foster innovation across a number of technologies. The explosion of data and computational capability has made advances in AI possible; but these resources are concurrently chokepoints preventing the maturity of the industry. Continued AI innovation will require large amounts of data and if the federal government provided more high-quality data sets to the public, entrepreneurs and researchers could compete more closely on the quality of their ideas, rather than their access to proprietary data sets. Open data does not just advance innovation, it can also promote equity by reducing one source of bias in AI—inferior training data. While vetted government data sets will not eliminate bias, this coupled with investment in digital infrastructure can go a long way in addressing digital equity. Whether it is increasing access to supercomputing resources for academic researchers to advance basic knowledge or providing broadband access so underserved communities can participate in the digital economy, the United States will not reach its full AI potential if bright minds are left behind.

Bringing these technologies into the public sector will also allow governments at all levels to better serve citizens. In the face of a global pandemic, government information technology systems at the federal, state, and local levels have been tested. When citizens needed government the most, paper-based processes and legacy digital systems failed to scale, causing unnecessary delays and suffering. Rapidly scaling capacity is just one benefit of moving to the cloud. With the public sector's data safely in the cloud, civil servants will be able to use modern tools, like those powered by machine learning and AI, to draw insights that were previously impossible. Armed with this new intelligence, civic leaders can offer Americans a better, more efficient version of government. The effort to modernize government systems should not cease after the coronavirus pandemic. Instead, we should use this as an impetus to supercharge modernization efforts.

While technology can be used to improve society, these same digital tools will be used against us by our adversaries. Russian disinformation operations have turned tools designed to bring us together into weapons to drive us apart. While the United States first experienced this in full force during the 2016 elections, many of its European allies, from the United Kingdom to Montenegro, have been dealing with the effects of Russian interference for years. In the summer of 2020, National Counterintelligence and Security Center Director William Evanina stated that not only did this malicious activity shows no signs of abating, but that countries like China and Iran were also starting to take a page out of the Russian playbook. In addition to disinformation, we have to be prepared for our adversaries' continued use of cyberattacks to steal intellectual property, probe critical infrastructure, and violate the privacy of Americans.

The next administration will be unable to tackle these challenges alone. Beginning with the Marshall Plan that rebuilt Europe after the Second World War and served as the bedrock commitment enabling the creation of NATO in 1949, the center of international prosperity and security has been U.S.-led alliances, not the United States alone. We stood up to despots and tyrants and helped our friends stand on their own. We did not take spoils but showed leadership and worked toward shared goals with our allies. If the next administration embraces the understanding that the United States has become an exceptional nation not because of what we have taken but because of what we have given, then we will continue our position as the global leader in advanced technology despite uncertain times.

November 2020

FOREWORD

CHRISTOPHER SCHROEDER

I am often asked about the most exciting developments in technology, and I like to cite the potential of artificial intelligence and data science, advancements in robotics and genomics, and more. But perhaps the greatest leap globally in technology is not the tech itself, but increasingly universal access to it. Ten years ago, analysts predicted that by 2020, two-thirds of humanity would have a smart device—each "phone" with more computing power than NASA had to put a man on the moon. Today most communities have blown through those predictions, dramatically expanding the ability of people everywhere to connect, collaborate, and learn. What is more, this shift has unleashed talent and innovation, forever changing who can compete in the new global economy, and how they do so.

The coronavirus pandemic has accelerated all these trends—perhaps ten years of technology adoption and embrace of digital life has happened in a matter of months. Compelled to buy daily staples online, attend virtual classes, and video chat with their doctors, millions have embraced behavioral changes that will only reinforce and intensify the speed of technological advancement.

That expanded access to technology is unleashing so much bottom-up innovation should not mask the top-down impact that governments and other institutions can have. It is tempting, especially in the business world, to hope these institutions merely "get out of the way," and sometimes they should. At the same time, the physical infrastructure, education systems, regulatory environments, and rule of law created by these institutions are at the center of what allows a society to survive and thrive in the midst of rapid change.

In the United States and around the globe, the stakes could not be higher. While billions of people have rapidly entered the digital age, millions in the United States lack access. We have long paid lip service to the "digital divide," and some efforts to bridge it have made progress. But in the 21st century, asking someone to work, live, and learn without the Internet is like asking them to get by in the 20th century without a road to drive on.

Since the Second World War, succeeding in the global economy has meant making technology in, or selling a product to, the United States. This assumption no longer holds. As innovative talent is unleashed in every country, globally competitive enterprises are being built everywhere. China is the prime example of a rising market that now stands toe to toe with the United States and it has succeeded by developing technology that is increasingly popular worldwide. And there are many "mini Chinas" rising: from Indonesia to Vietnam, Egypt to Kenya, Estonia to Brazil.

We are witnessing a new globalism, whether we wish to believe it or not. And we are in the earliest stages of these momentous shifts.

So where are these shifts discussed in the U.S. political debate? It is shocking that the answer is "almost nowhere." Not one question in the presidential debates focused seriously on the United States' place in global innovation, or how new tools will reshape how to learn, engage, heal, buy, or sell domestically. When technology does enter the political discussion, it is often treated as a side show, a ribbon-cutting PR event for politicians and nothing more. Or it is viewed solely for the threats it creates: from data breaches to political manipulation.

It is typical of Washington to look backward and try to drive policy change through old-fashioned models. Do we need a START treaty for cyberwar? Should fintech innovators be regulated under the regimes created for banking systems decades ago? This instinct is antithetical to the ethos of innovation. Washington cannot get caught in the tar of bureaucracy and regulatory constraint, lest we fail to achieve what citizens expect and our country needs.

What has been most seriously lacking is a coherent, cohesive, fact-driven analysis of where we are, what we want, and how we get there. We risk a haphazard approach with no overarching plan or vision for the future.

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) has leapt out as a leader in advancing innovation and increasing economic opportunity for all, while strengthening democratic values at home and abroad. The breadth and coherence of #Tech2021—honest, expert-led, digestible, and action-oriented—is astounding. It pushes us to stop sleepwalking toward predictable outcomes and offers ideas that will light up conversation in the United States and among its allies and partners.

Technology knows no party or border. U.S. leadership requires the will to move beyond political oversimplification and demands a grounding in the facts as we understand them, a coherent debate about 21st century strategy, and clear, actionable ideas that the next administration must prioritize. #Tech2021, in the end, is an inspiring call to action.

November 2020

INTRODUCTION

KAREN KORNBLUH, SAM DUPONT, AND ELI WEINER

Congressman Will Hurd and Chris Schroeder underscore in their forewords that the United States finds itself at a pivot point when it comes to innovation. New technologies will bring enormous new opportunity we must seize to address our existing challenges—and new disruption to which we must respond. Fortunately, good ideas abound for how to ensure these innovations improve lives, increase national security, and strengthen democratic values.

#Tech2021 offers strategic, turnkey reforms from experts for how the U.S. government can leverage technology to ensure individuals and society thrive in the midst of rapid change.

Despite the diversity of these briefs, some themes emerge:

- Innovation is fundamentally a bottom-up phenomenon, so opportunity to participate must be broadly distributed.
- As Schroeder observes, while many may wish for the government to simply "get out of the way," governments and other institutions working from the top down are needed to spur physical infrastructure (especially broadband access), education and training, and smart rules of the road that unlock the technological potential of our society and economy.
- Privacy protections and positive corrections to systemic inequities must be built in to ensure democratic values are protected and strengthened.
- Innovation happens in a global context. Democratic allies should work together to ensure that new technologies support and strengthen democratic values.

The ideas offered up are varied and specific.

Digital identities and resilient data architecture. Estonia's former president Toomas Ilves urges we learn from the Estonian model to improve the delivery of government services by creating a functional framework for digital governance. He urges two critical policy interventions: creating secure digital identities for individuals and creating resilient data architectures for government.

A national bank for green tech. Reed Hundt proposes closing the gap in funds needed to convert to 100 percent clean energy by financing catalytic investments that drive private capital toward a clean, technology-driven economy that creates new, high-paying jobs. A National Green Bank would focus on directly financing clean-energy projects, supporting state and local green banks, purchasing additional greenhouse-gas reductions, and ensuring a just transition.

A national open computing strategy. Lara Mangravite and John Wilbanks argue the government should provide subsidized cloud computing to lower cost barriers for scientific researchers to analyze large data sets and leverage its negotiating power to protect federal resources and the privacy of citizens whose data are analyzed.

Civic infrastructure for the 21st century. Ellen Goodman lays out an ambitious agenda for a building a 21st century civic information infrastructure through free or cheap broadband, digital distribution mechanisms to push information out to audiences, and protocols and tools to help users access data, verify information, and filter signal from noise.

Resilient tech supply chains. Edward Cardon, Harvey Rishikof, and Thomas Hedberg propose securing our critical technological supply chains by reforming the federal acquisition process. They urge mandating risk analysis and shifting the liability for security, encryption, and resilience to prime government contractors.

Safety locks for predictive analytics. Rashida Richardson offers three ideas for preventing the social harms posed by predictive analytics technologies: A moratorium and impact study on the validity of predictive analytics in government; transparency requirements including annual public disclosures of predictive analytics technologies acquired or used with federal funds; and algorithmic impact assessments of the risks of these technologies.

Watchdog accountability for privacy. Quentin Palfrey addresses our patchwork of privacy governance structures and accountability mechanisms with a three-part proposal: Baseline privacy rules modeled on the Fair Information Privacy Principles; increased accountability through law enforcement and digital privacy watchdogs; and training for developers based on an enforceable code of conduct

Updated work for a digital economy. Laura Taylor-Kale identifies three steps to bolster worker mobility and remove barriers to a more dynamic workforce: Universal broadband access, universal occupational licensing reciprocity, and greater portability of benefits—such as retirement, unemployment, paid leave, retraining and skill development, and childcare—from job to job.

A grand challenge for cyber risk statistics. Adam Bobrow argues that for cybersecurity to become a fully risk-based discipline, we need a Bureau of Cyber Statistics (as proposed by the Cyberspace Solarium Commission). He suggests a competition to prove the concept, which would include designing a set of metrics to measure cyber risk and developing a model that uses those metrics to accurately predict risk.

A digital trade agreement. Sam duPont suggests combatting the rising tide of digital trade barriers and ensuring a competitive global digital economy through a plurilateral digital trade agreement that combines high-standard rules on digital trade with deepened services commitments across the digital economy.

A national tech strategy cohort. Ian Wallace argues that if the United States is to pursue an industrial strategy it must hire, train, and support civil servants with the needed skill sets to generate and guide these policies. These leaders must understand the economic context for these policies, have a sufficient background in the relevant science and technology, and possess the strategic mindset and skills to leverage that knowledge in developing and implementing successful policy.

Digital financial infrastructure for fair finance. Tilman Ehrbeck and Kabir Kumar tackle the dated financial infrastructure in the United States that costs low-income Americans $2 billion in payday loans and $24 billion in bank overdraft fees each year. They propose reforms to create instant payments, digital identities, and a sound credit-scoring system to empower financial consumers.

Patent system transparency. Lisa Larrimore Ouellette and Heidi Williams propose creating a more favorable framework for innovation—even without resolving broader questions about the costs and benefits of patent protection—through clearer labeling of prophetic examples and increased transparency in patent ownership.

Principles to practice in AI governance: R. David Edelman sees risks if AI systems are deployed in socially significant situations before the technology is ready. Such failures will hurt individuals, harm society, and cause a crisis of confidence in the technology, undermining its potential. To avoid such an outcome, governments must undertake the hard, unglamorous, crucial work of translating ethical principles for AI into policy practice.

New incentives to tackle online disinformation. Karen Kornbluh urges changing platform incentives so that expectations for fairness from the analog world—for campaign finance transparency, consumer protection, civil rights, privacy, competition—are honored in the digital world. For this new system to work, platforms should implement a new circuit-breaker system to give them time to act. And a new PBS of the Internet should be created to support independent journalism.

These ideas can be implemented immediately. Doing so would improve lives, enhance innovation, and support rights. They do not require new federal agencies or a dramatic reorganization, simply a mainstreaming of technology and innovation into the working of government. In the coming months, we look forward to working with the next administration and Congress to do just that.

November 2020

UNLOCKING DIGITAL GOVERNANCE

TOOMAS ILVES

The Challenge: Government is Living in the Past

Almost every part of our lives is being digitized. You can buy a car, lease a house, find a doctor, and order groceries with a few taps on a screen. Our mechanisms of government, however, remain largely untouched by this digital revolution. Interacting with any level of government—local, state, or national—usually involves driving to a government office and standing in line.

Where it is possible to interact with the government online, doing so usually involves a shaky, dated, and insecure website, accessed using your email address and a likely hackable password. If your data is stored on a government server, you are left to wonder about the level of security. Data can be stolen, manipulated, or erased. Not infrequently, it is.

The Solution: Digital Identity and Data Integrity Can Unlock Digital Governance

Digital governance can update the apparatus of the state to meet the needs of the 21st century. In my native Estonia, secure and effective digital governance has increased access to public services, lowered barriers to citizen participation in civic life, enhanced the transparency of government agencies, and unlocked new areas of innovation. Digital governance only works, however, if trust has been established between the government and the citizen. Building this trust and reaping the benefits of digital governance require two critical policy interventions: secure digital identities for citizens, and resilient data architectures for governments.

National Digital Identity

Establishing a national digital identity program is the first step in creating a functional framework for digital governance. Simply put, a digital identity is the online persona of a subject; it ties an individual to a set of credentials across the Internet. The private sector has already recognized the power and potential of digital identities that are consistent across platforms. Apple, Facebook, and Google allow users to log into third-party websites and applications using their respective profiles. But for many of the services that digital governance makes possible, a Facebook account is not secure or verifiable enough. Government agencies must have a high degree of confidence that the digital persona claiming benefits or filing taxes is tied to the correct individual.

In Estonia, which boasts one of the first and most widely adopted national digital identity systems, citizens can cast a ballot, check medical records, establish a company, and sign legal documents using their state-issued digital identity. Authenticating themselves through either a physical ID card, a mobile phone, or a digital app, Estonians can access over 2,500 government services, as well as some private sector services such as banking. This two-factor authentication method guarantees the user's identity throughout their online interactions, saving time and resources for government and citizens alike—these savings total as much as 2 percent of GDP annually.[1]

Creating a national digital identity system requires care and caution. First, such a system must be secure and identities must be verifiable. Two-factor authen-

[1] e-Estonia Briefing Center, We have Built a Digital Society and We Can Show You How, undated.

tication—such as combining a password with a government-issued ID card—should be adequate for most services. For especially sensitive tasks like voting, biometric data—such as a fingerprint or facial recognition—may be necessary. The latest advancements in mobile phones and computers have made biometric authentication an increasingly prevalent and accepted form of identification.

Second, the digital identity must be portable and interoperable. The same digital ID must be sufficient for use across a variety of different platforms, services, and websites. Logging into the Department of Motor Vehicles should require the same set of credentials as applying for financial aid or state-level unemployment. This consistency is critical to widespread adoption.

Third, a national digital identity should enhance rather than encroach on privacy. In many cases, having a digital identity can prevent privacy violations by limiting the amount and type of data shared in online transactions. For example, rather than providing one's full date of birth, a digital identity could simply confirm that a user is over a specified age limit. Using a national digital identity as a primary method for accessing some private sector services (rather than a social media log-in) could also reduce the possibility of online tracking for advertising, removing certain tasks from the personal data economy.

National Data Architecture

Of course, digital identities offer trust and transparency only in one direction. While the government might be confident that it knows who a user is, the user must also trust that their data is being used appropriately. In addition to maintaining data security, national data architecture must also guarantee resiliency and integrity to ensure that trust flows both ways.

Data resiliency—ensuring that data systems cannot be destroyed or rendered inaccessible—is a critical aspect of national data architecture. In 2019, over 40 U.S. cities—including Baltimore, Atlanta, and New Orleans—were affected by ransomware attacks that crippled key municipal services.[2] These attacks undermine the ability of citizens to rely on digital governance. Estonia has established a data embassy in Luxembourg that provides redundant and secure data storage, ensuring that if a breach does occur, critical IT systems remain usable.

National data architecture must also guarantee data integrity—ensuring that data cannot be illicitly altered. This is a familiar challenge in Estonia. Twelve years ago, the country began putting all sensitive public data on a blockchain, making it impossible to alter data without express citizen assent while promoting individual privacy. When attacks are successful, knowing that data has not been modified helps ensure that trust endures.

Conclusion

If digital governance was once seen as desirable, the coronavirus pandemic has demonstrated its necessity. Debates about the legitimacy, efficacy, and feasibility of providing government services in the midst of a pandemic would be greatly mitigated by a system built from the bottom up with integrity, privacy, security, and resiliency in mind. Digital governance is now essential; to achieve it, the mechanisms of government must be rebuilt to fit the era in which we live.

[2] Manny Fernandez, David E. Sanger, and Marina Trahan Martinez, "Ransomware Attacks Are Testing Resolve of Cities Across America," New York Times, August 22, 2019.

November 2020

INVESTING IN THE FUTURE WITH A NATIONAL BANK FOR GREEN TECH

REED HUNDT

The Challenge: A Climate Crisis and Economic Emergency

The conjoined crises of climate change and the coronavirus pandemic have revealed the urgent need to pursue alternative avenues for innovation and investment. Extreme weather events cost the United States over $45 billion in 2019, while the pandemic has resulted in over 200,000 deaths in the United States and over a million worldwide. Today, as the west coast experiences devastating wildfires and the country suffers from high unemployment, the country must seize the opportunity to address both through national investment in green technology.

What the United States lacks today is not political will—climate change is no longer a partisan issue, with four of every five voters identifying it as a major crisis or real problem.[1] Rather, it lacks a functioning framework through which to channel this ambition. Direct government funding will not be adequate to meet the challenge: recent estimates suggest that converting to 100 percent clean energy would require $4.5 trillion in investment.[2] Instead, climate investment policies must be catalytic, driving private capital toward a clean, technology-driven economy that creates new, high-paying jobs. The solution lies in the creation of a National Green Bank.

The Solution: A National Green Bank to Invest in Clean Energy and Green Tech

Green banks currently exist at the state and local level. These smaller efforts have delivered outsized results, with the current roster of 15 catalyzing $5.3 billion in clean-energy investment since 2011. In 2019, every $1 invested by a green bank resulted in $3.60 of total investment into the U.S. clean-energy economy.[3] The model is working; all that is needed now is the ambition to implement it on a national scale.

Congress has recognized the need for a National Green Bank and sought to deliver it. The National Climate Bank Act of 2019, which has been introduced in the House and Senate, would establish an independent, non-profit entity capitalized with $35 billion in federal funds over six years.[4] The House passed the bill with a strong bipartisan vote in the summer of 2020. However, the bill was not taken up by the Senate and, now that this Congress is coming to a close, the legislation will have to be reintroduced in 2021.

Under this act, the National Climate Bank would be tasked with raising and deploying capital in order to maximize reductions in greenhouse-gas emissions, and with prioritizing projects that offer economic benefits to frontline and marginalized communities, which experience the first and worst impacts of climate change. Analysis by the Coalition for Green Capital suggests that the bank would be able to mobilize up to $1 trillion of investment over the 30-year length of its charter by drawing in private investment and recycling its initial capital.[5] A National Green

[1] Coalition for Green Capital, Polling Results, May 2020.

[2] Wood Mackenzie, Deep decarbonization requires deep pockets – trillions required to make the transition, June 11, 2019.

[3] American Green Bank Consortium, Green Banks in the United States: 2020 US Green Bank Annual Industry Report, 2020.

[4] House of Representatives, National Climate Bank Act (H.R. 5416), introduced December 12, 2019.

[5] Coalition for Green Capital, Mobilizing $1 Trillion Towards Climate Action, September 2019.

Bank, as proposed in the 2019 draft legislation, should focus on four categories of activity: directly financing clean-energy projects, supporting state and local green banks, purchasing additional greenhouse gas reductions, and ensuring a just transition.

Financing Clean Energy Technology

A National Green Bank should undertake direct financing of capital-intensive projects in a variety of sectors and technologies, including energy generation, transmission, and transportation. Low-cost financing for utility-scale renewable energy technology—such as solar, wind, geothermal, and hydropower—could help transform electric power generation, which still accounts for over 25 percent of U.S. greenhouse-gas emissions. By increasing the competitiveness of renewables and reducing project costs, a green bank could spur the uptake of clean energy in crowded markets and penetrate regions where renewable generation was previously nonviable. Similarly, the construction of a smart electrical grid, which is integral to the successful integration of renewables, is ripe for green-bank investment. A green bank should invest directly in transmission projects and invest in advanced battery technology, such as lithium ion-based batteries, and technically innovative storage systems, like gravity storage able to stockpile large amounts of intermittent energy by harnessing the earth's gravitational pull.

Meanwhile, transportation remains the highest contributor to U.S. greenhouse-gas emissions. A green bank should invest in the advancement of electric-vehicle technology and the charging infrastructure it requires. Additionally, it could drive investment in public transit, from bike-share programs to all-electric bus fleets. Beyond these sectors, a green bank should also direct capital toward climate-resilient infrastructure, industrial decarbonization, and energy-efficiency programs.

Supporting State and Local Green Banks

Many clean-energy projects require local expertise. Energy markets are regulated at the state level, and clean-energy market participants such as contractors and developers generally operate within a single jurisdiction. In these cases, a National Green Bank would be able to assist in two ways: by supplying seed capital and technical assistance to create subnational green banks where they do not already exist, and by providing a low-cost capital base for those that do so that they can undertake the financing of state and local initiatives. A National Green Bank should operate with an internal team specializing in the formation of green banks, offering technical assistance to remove barriers to growth in the green-bank ecosystem. For new and existing green banks, a National Green Bank should provide funding in the form of grants, loans, or loan guarantees.

Purchasing Additional Greenhouse-Gas Reductions and Ensuring a Just Transition

Furthermore, a National Green Bank should be authorized to accelerate the clean-energy transition by purchasing fossil fuels while they are still in the ground or paying coal plants to cease operation. Finally, a National Green Bank should be charged with remedying the long-term injustices and inequities that low-income communities and communities of color have disproportionately suffered from the burning of fossil fuels. Aside from merely delivering clean energy at competitive prices, it should prioritize investment—including investment in job training and reskilling—in communities that have suffered economically from the closure of fossil-fueled facilities or long-term negative health effects from living in high-pollution areas.

Conclusion

The benefits of a National Green Bank extend beyond achieving clean-energy objectives. A $35 billion deposit, once mobilized, would put millions of currently unemployed Americans back to work across every state. Voters want Congress to invest in clean-energy infrastructure and the jobs that come with it, with and over 80 percent of Democrats as well as over 50 percent of independents and Republicans embracing a National Green Bank as an engine of job creation and stable employment.[6] Solar and wind technology, smart electrical grids, Internet-of-Things-enabled charging infrastructure—all need to be built, and at a time when over 10 million Americans remain unemployed, there are workers ready to build them. All that remains is to create the financial vehicle ready to invest in them.

[6] Coalition for Green Capital, Polling Results.

November 2020

LEVERAGING OPEN DATA WITH A NATIONAL OPEN COMPUTING STRATEGY

LARA MANGRAVITE AND JOHN WILBANKS

The Challenge: Private Cloud Computing Hampers Open Data Efforts

Open data mandates and investments in public data resources, such as the Human Genome Project or the U.S. National Oceanic and Atmospheric Administration Data Discovery Portal, have provided essential data sets at a scale not possible without government support. By responsibly sharing data for wide reuse, federal policy can spur innovation inside the academy and in citizen science communities. These approaches are enabled by private-sector advances in cloud computing services and the government has benefited from innovation in this domain. However, the use of commercial products to manage the storage of and access to public data resources poses several challenges.

First, too many cloud computing systems fail to properly secure data against breaches,[1] improperly share copies of data with other vendors,[2] or use data to add to their own secretive and proprietary models.[3] As a result, the public does not trust technology companies to responsibly manage public data—particularly private data of individual citizens. These fears are exacerbated by the market power of the major cloud computing providers, which may limit the ability of individuals or institutions to negotiate appropriate terms. This impacts the willingness of U.S. citizens to have their personal information included within these databases.

Second, open data solutions are springing up across multiple sectors without coordination. The federal government is funding a series of independent programs that are working to solve the same problem, leading to a costly duplication of effort across programs.

Third and most importantly, the high costs of data storage, transfer, and analysis preclude many academics, scientists, and researchers from taking advantage of governmental open data resources. Cloud computing has radically lowered the costs of high-performance computing, but it is still not free. The cost of building the wrong model at the wrong time can quickly run into tens of thousands of dollars.

Scarce resources mean that many academic data scientists are unable or unwilling to spend their limited funds to reuse data in exploratory analyses outside their narrow projects. And citizen scientists must use personal funds, which are especially scarce in communities traditionally underrepresented in research. The vast majority of public data made available through existing open science policy is therefore left unused, either as reference material or as "foreground" for new hypotheses and discoveries.[4]

The Solution: Public Cloud Computing

It is necessary to extend existing commitments to open science by ensuring that cloud computing on open scientific data is as safe and inexpensive as possible. This commitment should be made not just

[1] Somayeh Sobati Moghadam and Amjad Fayoumi, "Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues," IEEE Access, vol. 7, 2019.

[2] DJ Pangburn, Despite the Controversy Plenty of Smaller Tech Startups Work-with ICE, Fast Company, October 4, 2019.

[3] Mark Harris, "How Peter Thiel's Secretive Data Company Pushed Into Policing," Wired, August 9, 2017.

[4] Christine Borgman and Irene V. Pasquetto, How and Why do Scientists Reuse Others' Data to Produce New Knowledge?, Cochrane Colloquium: Fringe Event, Edinburgh, September 15, 2018.

to academics, but to those with the lived experience represented in the data. The federal government can do this in the short term by negotiating on behalf of citizens for cloud computing, resulting in a deal that is inexpensive because of scale, and protective of individual privacy by contractual default. And it can accomplish this in the long term by creating a market competitor in cloud computing that operates on a "utility" business model that protects privacy and is optimized for U.S. scientific research.

By providing $1 billion in short-term vouchers to U.S. data scientists and investing another $1 billion to construct and operate a competitive public cloud computing platform, computing resources can be made available to all users who meet a minimum threshold of qualifications and agree to a social contract of open science ethics (for example, agreeing to respect restrictions on use in personally identifiable data). In so doing, it is possible to instantly increase the number of shots on goal against challenges related to biology and climate change. And by leveraging the negotiating power of the federal government, it is possible to protect federal resources and the privacy of citizens whose data are analyzed.

There is precedent for this proposal. The National Institutes of Health has recognized the potential of subsidized computing power to accelerate the use of data in the All of Us Research Program and the National COVID Cohort Collaboratory. In each of these large federal open data projects, deeply personal data about genetics and health are held in secure cloud repositories where users can visit the databanks, execute queries, upload their own data, and run exploratory analytics. They cannot however download the data, preserving the privacy of those represented and making oversight of data users more tractable.

But there is not yet a uniform policy or strategy to pair open data resources with low-cost, publicly available, privacy-protecting open data usage. Over the long term, the voucher model could address concerns associated with private cloud computing services by creating a public competitor that integrates privacy and security at a high level.

This proposal would also support equity and inclusion. Many researchers from communities underrepresented in data science are hamstrung by resource constraints that do not apply to wealthy, white communities. By easing resource constraints, the federal government can cultivate a generation of data scientists within those communities, empowered to explore questions and issues that are relevant to their own contexts and experiences.

Further, the proposal contributes to job creation. Public cloud vouchers will make it cheap and easy for entrepreneurs and community organizations to make data science a part of normal operations. These services will need to be staffed, representing an opportunity to cultivate jobs in data curation, cybersecurity, data analysis, and other areas, including in communities underserved by the knowledge economy. These jobs could be virtual and thus open to rural and urban communities across the country.

Conclusion

The benefits of a national open data computing strategy extend beyond getting processors humming on open data. Open data is desirable because it benefits individual citizens and the country as a whole. A $2 billion investment would immediately turbocharge the use of open data to solve challenges related to cancer, the coronavirus pandemic, social determinants of health, climate change, agriculture, and many other essential areas for resilience and innovation. This is the moment to accelerate U.S. data science.

November 2020

BUILDING CIVIC INFRASTRUCTURE FOR THE 21ST CENTURY

ELLEN P. GOODMAN

The Challenge: The Production of Authoritative Information is Drying Up

The United States is in the midst of an information crisis. Important news stories go unwritten, quality journalism is overwhelmed by clickbait, and the business model for trustworthy reporting has been decimated by social media's capture of advertising dollars. Since 2006, newspaper advertising revenue—which historically supported the production of high-quality journalism—has fallen by 50 percent, creating a hole that digital subscriptions are not even close to filling. At least 300 communities that once had a local newspaper no longer do. In 2019, Google made $8 billion more in advertising revenue in the United States than all local TV and radio stations combined.[1] At the same time that they are losing the funds to create journalism, independent media are also losing their direct relationship with citizens. Instead, news aggregators like Facebook and Google keep users on their own platforms with headlines and snippets for readers to skim.

The cost for democracy of this shift from a news producer-consumer relationship to a digital platform-user relationship is high. Local news production leads to increases in government accountability, voting, civic engagement, and overall democratic health.[2] But high-quality journalism is expensive, and if the profits of good reporting do not accrue to the outlets that produce it, these outlets cannot sustain their work. As one local newspaper editor put it: "If that cycle continues indefinitely, quality local journalism will slowly wither and eventually cease to exist."[3]

There are many excellent and urgent proposals to reinvigorate local journalism by pumping government and foundation funding into public-service journalism or by taxing digital platforms to pay for some of these efforts. Proposals from Free Press,[4] Save the News,[5] and other commentators,[6] as well as those contained in the Stigler Report,[7] prescribe important interventions to reinvigorate news. As important and necessary as such efforts are, they are only part of what is needed to sustain a civic information infrastructure.

Low-value information is crowding out real news. Even if the United States reinvests in public-service journalism, mere abundance cannot be relied on to

[1] U.S. House of Representatives, Subcommittee on Antitrust, Commercial and Administrative Law, "Investigation of Competition in Digital Markets," October, 2020.

[2] Amy Mitchell et al., "Civic Engagement Strongly Tied to Local News Habits," Pew Research Center, November 3, 2016; Mary Ellen Klas, "Less Local News Means Less Democracy," Nieman Reports, September 20, 2019.

[3] Statement of Kevin Riley, Editor, The Atlanta Journal-Constitution, quoted in House Antitrust Report, p. 61-62.

[4] Craig Aaron and S. Derek Turner, "What a Journalism-Recovery Package Should Look Like During the COVID-19 Crisis," Free Press, May, 2020; Timothy Karr and Craig Aaron, Beyond Fixing Facebook, February 2019.

[5] Save the News, "Save the News Senate Newspaper," 2020.

[6] See Victor Pickard, Democracy Without Journalism?: Confronting the Misinformation Society, Oxford University Press, 2019; Philip Napoli, Social Media and the Public Interest: Media Regulation in the Disinformation Age, Columbia University Press, 2019; Gene Kimmelman, "The Right Way to Regulate Digital Platforms," Harvard, Kennedy School, Shorenstein Center on Media, Politics and Public Policy, September 18, 2019.

[7] University of Chicago, Booth School of Business, George J. Stigler Center for the Study of the Economy and the State, "Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report," July 1, 2019.

ensure that high-value information wins the battle for attention. To be effective in informing the citizenry, journalism must be salient and trusted. It must be the signal that cuts through the noise. It must not simply be available to people, but be conspicuous in the flows of information that people consume. To be trusted, journalism must be worthy of trust because of its fact-based and public service principles, and it must also be seen as trustworthy through practices of transparency and data access. The creation of salience and trust will require efforts that penetrate through the full stack of information creation and distribution.

The Solution: A Full-Stack Approach to Civic Information Infrastructure

Inspiration can be drawn from past investments in public-service information infrastructure that go beyond the content layer to address other essential layers in the stack. These included investments in physical infrastructure like broadcast spectrum and satellite facilities. They included investments in distribution, ensuring that public-service media channels were actually received on broadcast receivers, and funding the transition to digital technology. The postal system also reflects a public investment in civic information infrastructure, as do the many state and local requirements that civic information be pushed out to citizens through notices placed in widely accessed media. An adequate 21st century civic information infrastructure will require government investment in physical access such as free or cheap broadband, digital distribution mechanisms to push information out to audiences, and protocols and tools to help users access data, verify information, and filter signal from noise.

Physical Infrastructure

The base layer of physical infrastructure provides the foundation that allows the rest of the stack to function. The digital-first format that characterizes 21st century media means that broadband must reach all members of the public, including those in rural areas, tribal territories, urban housing, and other underserved locations. Compared to their counterparts in other wealthy countries, Americans pay some of the highest rates for broadband while experiencing some of the slowest speeds.[8] The coronavirus pandemic exposed the fact that tens of millions of Americans lack access to adequate broadband to participate in distance learning and work.[9] A universal broadband guarantee, which treats broadband as a public good rather than a private endeavor, would lower barriers to access and make certain that public-service content is available to all.

Digital Distribution

The next layer up from physical access is digital distribution. Social-media platforms such as Facebook and Google are currently the principal gateways to civic information. If a government or journalist wants to reach people, they are beholden to these gatekeepers and their algorithms, and they have no meaningful direct access to users. Moreover, how content appears is likely to be de-contextualized and fragmented, as well as stripped of credibility cues and markers of trust.[10] Investment in marking information salient to civic needs—such as voting or public health information—and pushing that information out to people is important. More significantly, there should be public options that serve as alternatives to private tech oligopolies so that nonprofits, governments, and public-service entities do not have to rely on private actors to host their content. Any such public options should be interoperable with private alternatives to ensure that moving from one platform to another is transparent to the user.

[8] Becky Chao and Claire Park, "The Cost of Connectivity 2020," New America, last updated July 15, 2020.

[9] Linda Poon, "There Are Far More Americans Without Broadband Access than Previously Thought," Bloomberg, February 19, 2020.

[10] Journalism has increasingly become "atomized" and misleadingly embedded in other content. See Australian Competition and Consumer Commission, "Digital Platforms Inquiry," June 2019, p. 297.

Tools and Protocols

Making interoperability and salience markers work will require standards and protocols that return power to users. For example, users should be able to apply filters to social-media platforms to select for important, truthful information. Standards for interoperability can ensure that public options for content distribution can exist alongside private ones. Indeed, standards and interfaces that allow users to carry their social networks from one platform to another are the only way to decentralize networks, and decentralized networks have always been an aspiration of U.S. media policy. Beyond these pro-competition standards, protocols that help tag authoritative information, authenticate producers, marginalize deep fakes and other forms of misinformation, and supply trust signals will help to boost signal over noise.

Conclusion

What is needed is a 21st century civic infrastructure stack of interconnected and interoperable but independent layers, all of which work together to address the issues of production and distribution of public-interest media. By ensuring that well-funded public-access media are supported by a framework of universally accessible physical infrastructure, digital distribution that supports civic information, and standards and protocols that help consumers surface authoritative information, traditions of supporting civic information infrastructure can be carried into the digital era.

November 2020

MITIGATING SUPPLY CHAIN RISK: COMPONENT SECURITY IS NOT ENOUGH

EDWARD CARDON, HARVEY RISHIKOF, AND THOMAS HEDBERG, JR

The Challenge: Supply Chains are a National Security Vulnerability

As the United States has grown increasingly reliant on global supply chains, there has been renewed interest in their security. Because of the way supply chains developed globally over time, they are now more vulnerable to deliberate, malevolent interference, and more general trade disruption. These concerns have been exacerbated by the coronavirus pandemic. In addition, the definition of security for supply chains has also become quite broad, now including an array of concerns ranging from operational and financial security to cybersecurity and counterintelligence. Tolerance for supply-chain risks is decreasing as producers are recognizing the global complexity of supply chains, their fragility, and the increasing tensions with China. These characteristics create vulnerabilities and opportunities for blended attacks. The Department of Defense faces an operational imperative to build an integrated risk approach that addresses the blended vulnerabilities in supply chains.

Currently, most defense systems have hardware and software from multiple subprime vendors, and the focus has been on ensuring the provenance and security of each individual component. This approach rests on the assumption that secure individual components create secure overall products. But this assumption fails to account for larger integration challenges, which add an exponential level of complexity to any product or platform. A perfectly secure component can be compromised during assembly, especially if there are software-interface requirements introduced through programming and testing. In addition, the interfaces themselves can be compromised. Depending on what decisions were made earlier in a component's or system's life cycle, a compromise may not be detectable or corrected. New methods are required to address these challenges.

The Solution: A New Approach to Risk Integration for Defense Systems

To ensure supply-chain risk does not grow into a greater national security risk, a change in thinking is needed in the way major defense projects manage risk. For that to happen the federal government must propose, and Congress must pass, legislation that would shift a portion of responsibility for supply-chain risk to integrators—the prime vendors responsible for integrating complete products and systems—requiring these critical actors to ensure operational security of defense systems.

While the defense sector is not the only part of the U.S. economy subject to supply-chain risk, it is a good place to start in addressing vulnerabilities. The stakes in defense are high enough to overcome resistance to change, and defense and acquisitions processes are highly complex, presenting an opportunity to develop reforms that can be adapted to simpler contexts. Moreover, the defense budget is big enough to affect critical markets, helping spur second-order reforms. The federal government also has broad authority to act in matters regarding the defense sector.

This effort can build on recent positive developments. For example, the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) holds defense-industrial base (DIB) vendors accountable for cybersecurity. However, the CMMC lacks methods for holistically and systematically analyzing the security posture of the DIB. Even with the CMMC, questions remain over accountability, authority, and responsibility for the cybersecurity of the DIB and the government. Therefore, new legislation should resolve these questions by making prime vendors accountable for the overall security of each defense system for which they are under contract. Furthermore, the DIB should be required to do so by adopting a "system-engineering model" for risk that identifies the dependencies and interdependencies of relevant components and demonstrates that the integrated risks have been addressed.

Such a shift in the approach to supply-chain risk would require action across the Department of Defense, involving efforts in science and technology, research and development, and policy development. It would have even bigger implications for the defense-industrial base and its relationship with the Department of Defense. To work, the legislation would require two key components.

First, legislation should incentivize this shift in how system risk is managed. For example, financial instruments, tax incentives, insurance, and litigation all drive corporate behavior. A bond-like instrument and/or a bonus-like structure could hold capital for an appropriate amount of time after full-rate production and release it once the program risks are fully understood. The appropriate time would be determined based on the size, scale, and complexity of the program. This would give the research communities and government time to understand supply-chain and system integration risk management throughout the entire process.

Second, the government needs the capability to assess technical system integration and supply-chain risk. Therefore, a third-party technical-integration risk-assessment organization should undertake holistic system-engineering assessments to advise the acquisition, security, and intelligence communities in meeting their responsibilities. This organization could be led by a federally funded research and development center or university-affiliated research center acting as a trusted agent and would need to combine testing and evaluation with operational validation and verification at scale. It would need to be staffed with the appropriate level of critical expertise to provide an unbiased assessment.

These requirements would need to be fully funded, and the effort would carry a total cost of several billion dollars. But the long-term savings from more streamlined risk management practices— along with the benefits to national security—make this a small price to pay.

This solution would mitigate the risk of products and systems being developed that have major vulnerabilities, such as open test ports, open interfaces, and a lack of appropriate encryption levels. In the worst case, prime vendors make completely closed systems, which constrains the ability to continuously update those systems to minimize risk. Conversely, by incentivizing secure acquisition approaches such as resiliency, virtualization, containerization, and encryption, the federal government can support more secure practices that would benefit the government and the vendors. This approach would produce appropriately open, but secure, systems that can be rapidly upgraded (software and hardware) based on newly discovered vulnerabilities or threat actions.

Conclusion

Implementing such a fundamental change in supply-chain risk management requires strong and determined leadership. Current efforts focused on securing individual hardware and software components are not delivering supply-chain security—they are simply delivering component security. Bold action toward an integrated risk approach is needed for ensuring the security of the United States' critical defense systems.

November 2020

ADDRESSING THE HARMFUL EFFECTS OF PREDICTIVE ANALYTICS TECHNOLOGIES

RASHIDA RICHARDSON

The Challenge: Inequitable Consequences of Predictive Analytics Technology

Predictive analytics are information technologies that learn from historical data to predict future behavior or outcomes of individuals or groups to inform better decisionmaking.[1] They often employ data-mining techniques to identify patterns in large data sets and apply mathematical formulas to assess probabilities associated with different variables and outcomes. In commercial settings, predictive analytics enables recommendation features on entertainment services like Netflix, advertising platforms like Instagram, or shopping platforms like Amazon. However, its increasingly common use in the public sector creates problems in sensitive social domains.

In law enforcement, "predictive policing" technologies are used to predict where a crime may occur or who may be a victim or perpetrator of a crime in a given window of time, yet the technology's reliance on biased police data can lead to its predictions perpetuating discriminatory practices and policies.[2] In housing, coordinated entry assessment tools are used to predict vulnerability within the underhoused population to prioritize allocation of housing assistance opportunities (such as emergency shelter or permanent supportive housing), but research has demonstrated that the most prominent tool is biased against Black, Indigenous and people of color individuals.[3] In child welfare, predictive risk-modeling tools are used to predict maltreatment by caregivers to inform decisions made by agency workers; but biased agency data and predictive variables lead these tools to assign higher risk scores to poor and minority families, which results in negative or punitive actions.[4] Since predictive analytics necessarily relies on historical data, when it is used in sectors with complicated social contexts and histories, the technology runs a high risk of reproducing and reinforcing historical practices, policies, and conditions. Compounding these concerns is the fact that the predictions produced by these technologies are generalizations, rather than the individualized assessments that should be considered for consequential decisions—like whether to provide temporary housing or to remove a child from a home.

Currently there are no laws or regulations to govern the design and use of predictive analytics technologies. The lack of constraints means that important societal questions—such as what to predict, what variables to include in prediction algorithms, the weight assigned to each variable, and standards for accuracy—are left to the discretion of engineers and data scientists and not subject to any form of public accountability. These concerns are exacerbated by the fact that the risks posed by predictive analytics technologies are not always immediately apparent, and there are often legal and practical impediments to

[1] Eric Siegal, Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, Wiley, 2016.

[2] Rashida Richardson, Jason M. Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," New York University Law Review Online, 2019.

[3] Catriona Wilkey et al, Coordinated Entry Systems: Racial Equity Analysis of Assessment Data, C4 Innovations, 2019.

[4] Virginia Eubanks, Automating Inequality: How Hight-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press, 2018.

redressing harms. For example, in law enforcement, housing, and child welfare, individuals harmed by decisions made using predictive analytics would not initially know that a technology was used in decision-making. Additionally, traditional means of redress, such as administrative appeals, may be ill-suited for mitigating the legal concerns posed by predictive analytics due to the lack of transparency regarding how these technologies work and the novelty of their use in the public sector.[5]

The Solution: Leveraging Existing Policy Approaches for High-Risk Technologies

Since the implications of predictive analytics technologies can vary across sectors, initial policy interventions must be diagnostic or investigatory, but also responsive to immediate concerns. The following three proposals are derived from existing draft legislation targeting high-risk technologies, and each attempts to leverage pertinent information to inform and identify long-term solutions.

Moratorium and Impact Study on Long-Term Validity of Predictive Analytics in Government

Considering the immediate and varied harms associated with the current use of predictive analytics in the public sector, a moratorium should be established to mitigate further harm.[6] This legislative intervention should also require and fund an impact study on the use of the technology within government, the potential benefits and risks, issues that require further study before government use is permissible, and recommendations to address challenges and opportunities.[7] The impact study should be co-led by the Government Accountability Office and the National Institute of Standards and Technology, and it should require consultation with experts and local communities where predictive analytics have been in use.

Transparency Requirements

While evidence of predictive analytics use within various government sectors is emerging through investigative reporting,[8] research,[9] and some official disclosures,[10] the full spectrum of uses within federal, state, and local governments remains uncertain. Thus, legislation should mandate annual public disclosures of predictive analytics technologies acquired or used with federal funds along with details regarding use and outcomes.[11] Such transparency requirements can offer insightful information about the prevalence and impact of this technology.

Algorithmic Impact Assessments

Algorithmic impact assessments seek to evaluate the risks of data-driven technologies by combining public agency review and public input to inform necessary safeguards to minimize risks.[12] Such assessments have been implemented in Canada[13] and there are U.S. legislative proposals[14] that include this intervention, though some are targeted at commercial entities rather than government agencies. Complementing the above proposals, algorithmic impact assessments offer useful information about the potential benefits

[5] Robert Brauneis and Ellen P. Goodman, "Algorithmic Transparency for the Smart City," Yale Journal of Law & Technology, 2018.

[6] See, for example, S.4084 – Facial Recognition and Biometric Technology Moratorium Act of 2020, Congress, introduced June 25, 2020.

[7] See H.R.6929 – Advancing Facial Recognition Act, Congress, introduced May 19, 2020; and H.R.827 – AI JOBS Act of 2019, Congress, introduced January 28, 2019.

[8] Kathleen McGrory and Neil Bedi, "Pasco's Sheriff Created a Futuristic Program to Stop Crime Before it Happens. It Monitors and Harasses Families Across the County," Tampa Bay Times, September 3, 2020.

[9] Catriona Wilkey et al, "Coordinated Entry Systems.

[10] Alleghany County, Alleghany Family Screening Tool, 2020.

[11] See S.2689 – No Biometric Barriers to Housing Act of 2019, Congress, introduced October 23, 2019.

[12] Dillon Reisman et al, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability, AI Now Institute, 2018; and Ansgar Koene et al, A Governance Framework for Algorithmic Accountability and Transparency, European Parliamentary Research Service, European Parliamentary Research Service, 2019.

[13] Government of Canada, Algorithmic Impact Assessment Webpage, 2020.

[14] See S.1108 – Algorithmic Accountability Act of 2019, Congress, introduced October 4, 2019; and S.2637 – Mind Your Own Business Act of 2019, Congress, introduced October 17, 2019,

and challenges of predictive analytics. They should also incorporate public consultation and require government agencies to proactively assess the necessity of formal policies and safeguards to mitigate risks.

Conclusion

Government decisions that are likely to seriously impact individuals' lives should not be made in a black box. Preventing the harms of predictive analytics will require the study of the technology's use and potential for abuse, strict transparency obligations when it is used, and impact assessments of predictive algorithms. The onus must be on the government to prove that the tools it uses do not exacerbate past and present inequities if we are to allow these technologies to contribute to public decisionmaking.

November 2020

ADVANCING DIGITAL TRUST WITH PRIVACY RULES AND ACCOUNTABILITY

QUENTIN PALFREY

The Challenge: A Governance Gap for Digital Privacy

The open nature of the Internet has given billions of people access to information and connected them in ways that had never before been possible. This free flow of information has enabled digital technologies to transform the economy and society, but it also creates unique governance challenges. Increasingly, the patchwork of governance structures and accountability mechanisms seem outmatched by the challenges that emerge from the digital landscape. The result is a governance gap that leaves users exposed to considerable privacy risks. Large majorities of Americans believe that they have very little to no control over the data that companies collect about them (81 percent) and are concerned about how companies use their personal data (79 percent).[1] Lack of trust in privacy protections threatens to undermine the promise mobile technologies offer to improve people's lives. For instance, last year, just over half of Americans (52 percent) decided not to use a product or service due to privacy concerns.[2]

Businesses are also inhibited by the current labyrinth of privacy rules. It is maddeningly difficult for developers and publishers seeking to offer digital products worldwide to know what the relevant rules are. Just within the United States, service suppliers must comply with jurisprudence governing unfair and deceptive trade practices under federal and state laws, individual state privacy laws in places like California and Illinois, and the latest terms of service of platforms such as Apple, Google, Facebook, Twitter, and Amazon. Even diligent, well-trained publishers seeking to follow the rules quickly find unnavigable murkiness as well as huge gaps and inconsistencies. The solution lies in creating systematic accountability structures that ensure users can trust their data will be treated with respect, and that provide certainty to online businesses.

The Solution: New Rules and Increased Accountability to Meet the Speed of the Internet

Governing the Internet presents unique challenges relating to complexity, time scale, and its global nature. Internet governance works best when legislatures pass broad rules, allowing technologists and specialized agencies to iron out specific rules. A new system for commercial data privacy must ensure that regulations move at the speed of the Internet.

Baseline Privacy Rules Modeled on the Fair Information Privacy Principles

In order to address the problem of the patchwork of U.S. privacy laws, Congress must pass baseline federal privacy protections modeled on the Consumer Privacy Bill of Rights (CPBR) framework developed by the Obama administration. Privacy norms must be established at the federal level, but any preemption of state laws such as California's Consumer Privacy Act should ensure that current consumer protections in state law are the floor, not the ceiling. Comprehensive privacy legislation at the federal level should include enforceable codes of conduct and robust accountability mecha-

[1] Brook Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control over their Personal Information, Pew Research Center, November 15, 2019.

[2] Andrew Perrin, Half of Americans have Decided Not to Use a Product or Service because of Privacy Concerns, Pew Research Center, April 14, 2020.

nisms. A law should include privacy principles based on the Fair Information Practices Principles, and specific rules should be fleshed out through multi-stakeholder processes that lead to enforceable codes of conduct.

Globalized data flows necessitate international cooperation. The U.S. government should lead efforts to harmonize privacy rules across jurisdictions. A Track 1.5 process could help lay the groundwork for more formal coordination and harmonization. Federal funding should support initiatives that prioritize multi-stakeholder collaboration around issues of Internet governance that consider the needs of developers, platforms, and users alike. Any U.S. privacy legislation should incentivize this process, such as new sources of liability coupled with a safe harbor for companies that follow codes of conduct reached through multi-stakeholder processes.

Increased Accountability through Law Enforcement and Digital Privacy Watchdogs

Law enforcement and consumer protection agencies such as the Federal Trade Commission and state attorneys general need ample resources to enforce the law. Congress should give greater resources to traditional law enforcement agencies such as the Federal Trade Commission for privacy enforcement. State attorneys general should be granted enforcement authority for the CPBR in connection with any preemption rules.

Law enforcement authorities need nimble, technically savvy partners such as nonprofit watchdogs to ensure accountability under circumstances that do not easily fit within a traditional law enforcement or regulatory structure.[3] Digital privacy watchdogs can help monitor and hold accountable privacy violators across the digital ecosystem. These watchdogs address a critical gap in digital accountability mechanisms, especially where bad practices do not necessarily require law enforcement but nonetheless erode customer trust in the mobile app marketplace.

In addition, the U.S. government should create a dedicated federal role of chief privacy enforcement coordinator whose mandate would include coordinating government agencies and activities. Creating such a role would be a significant move in the direction of prioritizing data privacy initiatives at the federal level. This position could be modeled after the role of the intellectual property enforcement coordinator and be based in the White House. Once implemented by statute, the chief privacy enforcement coordinator should provide periodic reports to Congress.

Training for Developers Based on an Enforceable Code of Conduct

A compulsory developer education and certification program would raise the bar on compliance and prevent problems before they cause risks and harms to users, or litigation and public relations risks for companies. Companies should be required by statute to ensure that developers on their platforms are trained in a curriculum that is based around an enforceable code of conduct. To support international consistency, that code of conduct should be consistent with the EU's General Data Protection Regulation and new U.S. privacy legislation. Any training requirements should be guaranteed through platforms' terms of service.

Conclusion

Digital technologies hold incredible promise to improve citizens' lives. Governing these tools, however, requires new thinking and new governance structures. The U.S. government has, so far, been unable to provide consumers with meaningful privacy protections, while companies are burdened with navigating complex, outdated rules. Accountability structures must ensure that users trust the digital tools available to them—but these structures should not be left to any one law or law enforcement entity. A system of privacy laws, government agencies, watchdogs, and developer education programs should work together to prevent, monitor, and hold accountable privacy violations, ensuring the digital ecosystem flourishes and consumers have effective advocates.

[3] Quentin Palfrey, "Watching the Watchers: More Accountability Needed to Ensure Responsible COVID-19 Tracing Tech," The Hill, July 13, 2020 .

November 2020

PRIORITIZING WORKFORCE MOBILITY IN THE AGE OF DIGITAL TRANSFORMATION

LAURA TAYLOR-KALE

The Challenge: Structural Barriers to Mobile Work and an Agile Workforce

When policymakers and pundits talk about the "future of work," most of the conversation focuses on the risk that automation and artificial intelligence pose to jobs. Indeed, these technologies necessitate that workers have higher technical and social skills. While these shifts will bring changes and challenges for workers, the digitalization of the economy creates tremendous opportunities as well. As cloud-based enterprise platforms and app-based services become more common, new digital business models are arising and ever more goods and services are becoming digitally deliverable. These shifts are creating a tremendous opportunity for workers to increase their mobility, agility, and freedom. The coronavirus crisis has accelerated these trends as digital connectivity has offered a lifeline to workers and businesses that can operate without a physical presence.

Building on these trends toward all-digital business models and a more mobile, agile workforce will yield significant benefits for workers and the United States as a whole.[1] Where digitalization allows workers to consider job openings across the country, their opportunities will broaden while employers' talent pools will become stronger and more diverse. Where digitalization allows workers to perform the same job from anywhere, they will benefit from the freedom to live where they please, and regions that have seen economic stagnation may attract new talent, commercial activity, and tax revenue. And where professionals can offer their services electronically, they can grow their client base and customers will have a broader set of service providers to choose from.

But three major barriers are holding back the further growth of worker mobility in the United States. First is the lack of universal broadband. Clearly, participating in almost any kind of remote work requires a strong, reliable Internet connection, and regions that lack broadband availability will be left behind. Second, antiquated state-level occupational licensing requirements present a significant obstacle preventing people from moving or accessing flexible work opportunities. Third, the system of tying benefits—particularly healthcare—to full-time employment makes it challenging and expensive for workers to take risks, change jobs, and work independently. Successfully addressing these challenges will leave the U.S. workforce far better equipped to compete globally in a digital age.

The Solution: Three Reforms for Workforce Mobility

To overcome the barriers preventing a more dynamic workforce, leaders must pursue three reforms in concert: universal broadband access, universal occupational licensing reciprocity, and greater portability of benefits from job to job. These reforms cut across diverse areas of policymaking and will require partnerships across government, businesses, and nonprofits. But the potential benefits—for workers, for businesses, and for U.S. competitiveness—are immense.

Universal Broadband Access

Broadband Internet is vital to our lives today. However, millions of Americans still do not have the access that they need in order to attend school online

[1] Edward Alden and Laura Taylor-Kale, The Work Ahead: Machines, Skills, and U.S. Leadership in the Twenty-First Century, Council on Foreign Relations, April 2018.

or work remotely. Tens of millions lack any access to broadband[2] and, even when access is nominally available, close to 160 million do not use the Internet at broadband speeds.[3] The federal government has recognized the need for building connectivity infrastructure, particularly as the pandemic shifted much of the educational system online. Earlier this year, the Federal Communications Commission launched the $20 billion Rural Digital Opportunity Fund with the goal of connecting millions of rural households to broadband.[4] But it is time to start thinking of high-speed Internet access as an essential service like water, electricity, or sanitation. The federal government should support efforts to expand the financing and construction of low-cost broadband infrastructure for all, building on the Broadband Infrastructure Finance and Innovation Act of 2019.[5] The future of work has no future at all if broadband remains out of reach for millions of would-be mobile workers.

Universal Occupational Licensing Reciprocity

Occupational licensing presents a significant obstacle preventing Americans from moving or accessing mobile work opportunities. Most occupational licenses are issued under the authority of state and local governments. Licensure is often required for a wide range of professional occupations, including for teachers, lawyers, physicians, pharmacists, dentists, real estate brokers and appraisers, barbers and cosmetologists, insurance agents, paramedics, and accountants. Roughly 25 percent of workers today require a state license and, more often than not, licensure is state-specific: a barber licensed in one state cannot cut hair in another without a burdensome relicensing process.[6] Economists estimate that state licensure regimes reduce interstate migration by as much as 36 percent, and disproportionately affect populations that most need to be mobile.[7] Since the onset of the coronavirus pandemic, this structure of state-by-state licensing has become an obstacle to public health and safety, leading to shortages in qualified health practitioners and impeding innovative business models like telehealth platforms.

The federal government should encourage state and local governments to implement licensing reciprocity. In 2017, the National Governors Association and the National Conference of State Legislatures launched efforts to improve the portability of occupational licenses for 34 occupations across 11 states.[8] These efforts have yielded some victories: in 2019, Arizona and Pennsylvania enacted laws recognizing universal out-of-state licensure for qualified professions, and a handful of states have enacted state-to-state reciprocity arrangements.[9] During the pandemic, several states implemented executive orders to temporarily waive licensing requirements for healthcare practitioners and allow telehealth practice.[10] However, these efforts have been piecemeal. While licensing regimes are important, protecting public health and safety from potential harm, too often these regimes have served as unnecessary barriers to mobility and impeded digitalization of many professions at a time when workers most need flexibility. The federal government should spearhead an effort to promote universal licensing reciprocity; each additional state that adopts such a measure will generate manifold benefits for workers, employers, and the economy as a whole.

[2] Federal Communications Commission, 2020 Broadband Deployment Report, April 24, 2020.

[3] Shelley McKinley, Microsoft Airband: An Annual Update on Connecting Rural America, Microsoft, March 5, 2020.

[4] Federal Communications Commission, FCC Launches $20 Billion Rural Digital Opportunity Fund To Expand Rural Broadband Deployment, January 30, 2020.

[5] U.S. House of Representatives, “Broadband Infrastructure Finance and Innovation Act of 2019 (H.R.4127),” introduced on July 30, 2019.

[6] Janna E. Johnson and Morris Kleiner, Is Occupational Licensing a Barrier to Interstate Migration?, Federal Reserve Bank of Minneapolis, December 6, 2017.

[7] Ibid.

[8] National Governors Association, 10 Transformational Pathways for States, accessed on November 6, 2020.

[9] Iris Hentze, 2019 Trends in Occupational Licensing, National Conference of State Legislatures, January 9, 2020.

[10] Carl Sims, Occupational Licensing – COVID-19 Responses, The Council of State Governments, April 6, 2020.

Portable Work-Based Benefits

Existing policies tie a wide range of benefits—including those for retirement, healthcare, job training, sick and family leave—to full-time employment. These policies are outdated in the digital economy. With the rise of digital business models and accelerated by the onset of the pandemic, more Americans need to be mobile to find meaningful work opportunities. But when benefits are tied to work, it is difficult for workers to leave their jobs, take risks, or work part-time. This system also creates particular harms for part-time and contingent workers whose jobs may not carry benefits at all. The Affordable Care Act is a step in the right direction in ensuring that workers have healthcare access independent of their jobs. Some workers, particularly minorities, value job security over mobility, and may not prioritize the portability of benefits, relative to other reforms, [11] but there is still ample room for improvement.

U.S. leaders should seek to establish portable systems of retirement, unemployment, paid leave, retraining and skill development, and childcare benefits tied to individual employees rather than solely to full-time jobs. Various proposals have been floated on how to construct portable benefits, including shared security accounts with employer prorated pay-in and pilot projects for institutions willing to experiment. Motivated by the coronavirus pandemic, Senators Mark R. Warner (D-VA) and Steve Daines (R-MT) introduced bipartisan legislation in July 2020 proposing an emergency portable benefits fund.[12] Passing a permanent version of this bill would be a very good next step toward making portable benefits more broadly available.

Conclusion

Digitalization has created opportunities for more mobile, flexible work, yet analog-age policies serve as barriers to Americans seeking new opportunities. The coronavirus pandemic only heightens this tension. To knock down these barriers, the White House should create a National Commission on the U.S. Workforce that brings together governors and mayors with senior officials in the federal government. This commission should work to identify and implement reforms to support the development of the workforce, including in the areas identified above. This kind of collaborative national effort will be essential to seizing the opportunities of the digital age for workers, companies, and the country as a whole.

[11] Ismail White and Harin Contractor, Racial Differences on the Future of Work: A Survey of the American Workforce, Joint Center for Political and Economic Studies, July 24, 2019.

[12] Office of Senator Mark Warner, Warner & Daines Introduce Legislation to Establish an Emergency Portable Benefits Fund, July 22, 2020.

November 2020

LAUNCHING A CYBER RISK GRAND CHALLENGE

ADAM BOBROW

The Challenge: Cyber Risk Must be Quantified

Across the economy, organizations are under serious pressure from cyber criminals, ransomware attacks against the healthcare sector are running rampant during a global pandemic, and hostile foreign actors have again sought to disrupt U.S. election infrastructure. Yet, cybersecurity still lacks the quantification needed to become a fully risk-based discipline. As a result, cybersecurity teams in organizations can report their good days––those on which no incident occurs––only by measuring how they updated a firewall or conducted anti-phishing training. Those reports do not connect with the question executives want answered: Have those activities reduced the risk faced by the organization? Connecting a cybersecurity team's activities with risk reduction will require measuring risk in quantitative terms. Industry and government leaders need new risk-measurement methodologies to make meaningful comparisons across industries and to direct appropriate interventions. There is no time to waste.

There are a number of reasons for the current lack of progress toward quantification. The private sector fears it will incur liability through information sharing, there is no agreed methodology about what data to collect and how best to collect it (including the right balance of quantitative alongside qualitative methods), and the cyber insurance industry has not been incentivized to apply the effort required to price cyber risk.

To overcome these challenges, the U.S. Cyberspace Solarium Commission proposed the establishment of a Bureau of Cyber Statistics (BCS), a data agency akin to the Bureau of Labor Statistics. The commission stated that establishing a BCS would be the best way to address the "lack of clarity about what security measures are effective in reducing risk [by] identifying and establishing meaningful metrics and data necessary to measure cybersecurity and risk reduction in cyberspace."[1] Support is growing in Congress for this proposal and the parallel recommendation to establish a public-private partnership on modeling cyber risk. Still, a pilot demonstration of the BCS concept would help build further support while also providing a foundation for a future federal BCS.

The Solution: A Grand Challenge for Cyber Risk Measurement

To build support for a federally-funded BCS and ensure the BCS has a positive impact on the cybersecurity ecosystem from day one, the federal government should take advantage of authority already available through the America Competes Act of 2007 to establish an open innovation competition—a "grand challenge"—to prove the BCS concept. The organizers should construct a competition that has two components: the design of a set of metrics to measure cyber risk and the development of a model that uses those metrics to accurately predict such risk. If successful, the competition would provide insight into what data sets best enable predictive models and provide the starting point for continued refinement of the most successful risk models, both of which would help inform the activities of the BCS. These metrics

[1] U.S. Cyberspace Solarium Commission, "Report," March 2020.

and models could be shared with the government to lay a foundation for the BCS.

Participation from the broader risk-management community would engage the wealth of knowledge and expertise available throughout the economy in developing the BCS. Participants might include representatives from industries such as insurance and cyber defense as well as academics and other risk professionals—potentially in cross-disciplinary teams. To encourage participation, all the teams would have the opportunity to commercialize their methods after the competition. The competition could also start building the case for private-sector companies to share their incident data with a trusted third party like the BCS, including the opportunity to benefit from the predictive models that sharing would make possible.

A key element of this competition would be ensuring that participants have access to the right data to develop cyber risk models. In the context of establishing the competition, one or more sector-specific information security and analysis centers/organizations (ISAC/ISAOs) could be charged with establishing a mini-BCS to generate the initial data sets. The sectors chosen would need to be those where members were willing to share cyber-incident data—either because they have a pressing need for analysis to help respond to such incidents (such as the healthcare sector) or because there exists little competitive motivation to prevent sharing information (such as state governments). Seed funding would enable the relevant ISAC/ISAOs to pilot the collection and curation of the incident data that competition participants would need to build models for quantitative cyber risk assessments.

The competition could be run by a number of federal government agencies that have been given the authority to do so under the America Competes Act. Perhaps the most obvious candidate would be the General Services Administration's (GSA) Challenge.gov program. The GSA would likely benefit from support from cybersecurity agencies like the Cyber and Infrastructure Security Agency within the Department of Homeland Security, which could play an important role in recruiting ISACs to capture and curate data. In the interests of building enthusiasm for the competition, however, the government might also seek to work with outside partners, including philanthropic donors to boost a potential prize pot and industry organizations to encourage private-sector participation.

Conclusion

The BCS is an important idea, and the need is pressing. There should be urgent action to prove the concept (and thus get the congressional and administration support it needs) and ensure that it hits the ground running. A grand challenge that attracts the finest risk management experts in the country is the best way to do that.

November 2020

STRENGTHENING THE GLOBAL INTERNET WITH A DIGITAL TRADE AGREEMENT

SAM DUPONT

The Challenge: Rising Barriers to Digital Trade

Around the world, governments are building digital walls by restricting the free flow of data, blocking online services and content, and fragmenting the Internet along national boundaries. The Chinese government was in the vanguard of this trend and has successfully pushed other governments to follow its lead in exerting greater top-down control over digital spaces. In 2020, Freedom House documented a tenth consecutive year of global decline in "internet freedom,"[1] and the Office of the U.S. Trade Representative documented a growing list of barriers to digital trade.[2]

These digital trade barriers do not just harm giant tech companies: from cloud computing, to insurance, entertainment, architecture and design, service suppliers across the economy need to move data across borders. Meanwhile manufacturers, farmers, and small businesses of every kind depend on digital services to operate and compete; sometimes these services are available from a local firm, often they are international. For the United States, the world's leading exporter of services, the commercial importance of an open, global Internet should be obvious. And authoritarian digital rules are not just bad for U.S. exporters: an Internet that is top-down, closed, and government-controlled hampers free speech and undermines the ability of governments and institutions to respond to global challenges with global coordination.

As international rules to govern the Internet are written in the coming years, the United States and its democratic allies must take the lead in creating a global framework that favors an open digital ecosystem.

The Solution: Negotiate a Digital Trade Agreement

Digital Trade Rules

To combat the rising tide of digital trade barriers and ensure a competitive global digital economy, the next administration should launch and lead negotiations toward a plurilateral digital trade agreement. The core of such an agreement should be high-standard rules on digital trade that allow businesses to operate globally and reach customers beyond their borders. Free trade agreements negotiated in the past ten years can serve as a model: they have included rules ensuring the free flow of data and prohibiting data-localization requirements, banning tariffs and discriminatory policies affecting foreign digital products, and protecting against unfair requirements to transfer source code or sensitive algorithms to governments.

Over the past three years, a growing group of members of the World Trade Organization (WTO) have been engaged in negotiations on digital trade rules. Many countries have engaged in good faith, but the participation of China, Russia, and other authoritarian governments makes a useful outcome unlikely. China, for one, has used the negotiations to advocate for its "Internet sovereignty" and oppose enforceable rules on core issues.[3] These negotiations have, however, high-

[1] Adrian Shahbaz and Allie Funk, Freedom on the Net 2020: The Pandemic's Digital Shadow, Freedom House, October 2020.

[2] Office of the United States Trade Representative, Fact Sheet on the 2020 National Trade Estimate: Strong, Binding Rules to Advance Digital Trade, March 2020.

[3] World Trade Organization, Joint Statement on Electronic Commerce: Communication From China, April 23, 2019.

lighted broad interest in defining rules to govern digital trade, and provided valuable information about various governments' positions and priorities on key issues.

Digital Services Commitments

In addition to defining rules for digital trade, an agreement should also ensure that service suppliers across the economy—not just the firms we think of as tech companies—can access foreign markets and compete on a level playing field. Given that nearly every service industry is digitally enabled, it makes sense that digital trade negotiations should provide benefits across the services sector. Establishing a large open market for service suppliers from participating countries would help counteract the unfair advantages China provides to its own firms. Additionally, such breadth may be necessary to ensure that the outcome complies with the rules for plurilateral agreements under the WTO's General Agreement on Trade in Services.

From 2013 to 2016, a group of 26 countries participated in negotiations toward a Trade in Services Agreement (TISA). While these negotiations stalled after President Donald Trump's election, TISA can provide a useful foundation for further negotiations. It also provides a good starter list of countries that may be eager to engage in digital trade negotiations. These negotiations should be open to any government that shares a genuine interest in a free, fair, and global digital economy as well as a willingness to negotiate in good faith and abide by enforceable, high-standard rules. This inclusiveness will help ensure that any agreement expands the bloc of countries committed to liberal digital governance, rather than ceding large swaths of the globe to China's influence.

Stumbling Blocks and Innovative Approaches

Any worthwhile negotiations take time, and this subject would be no exception. While these negotiations would avoid some of the trickiest areas in trade—such as agriculture and intellectual property—the intersection between data flows and data privacy has proven contentious in previous negotiations. This is one area where negotiators should aim to go further than past agreements and set baseline standards for the protection of consumers and their personal data. Ensuring data privacy among participating countries would help assuage some concerns about guaranteeing the free flow of information across borders. If Congress passes a federal data privacy law, the negotiators' task will be significantly eased.

These negotiations also present an opportunity for the United States and its partners to innovate new approaches to transparency in trade negotiations. Trade negotiations have historically been conducted largely in secret, frustrating stakeholders that wish to provide input. This opacity may have eased negotiations, but it has made the politics of trade more difficult. Given the subject matter of digital trade negotiations, participants might wish to experiment with using digital technology to facilitate their transparency.

Conclusion

The United States and its democratic partners have a strong interest in an open, global information ecosystem that defaults toward free competition, the free exchange of ideas, and the free flow of data. The U.S. government needs to rediscover its leadership in advancing this vision, but it cannot do so alone. The United States and the European Union share democratic values and a commitment to market-based economics; if they are able to bridge their differences on digital trade, they could define a democratic model—and an alternative to China's approach—for the many other governments that are weighing their options.

November 2020

ESTABLISHING A TECH STRATEGIST COHORT ACROSS THE FEDERAL GOVERNMENT

IAN WALLACE

The Challenge: The United States lacks the talent to guide an industrial strategy

The United States is moving toward a more overt industrial strategy. The federal government has long played more of a role in guiding the economy than politicians have been comfortable admitting. But with China emerging as a peer competitor in critical and emerging technologies and a growing need for action on climate change, the taboo on industrial policy is disappearing and making more activist strategies politically possible.[1] Yet while support for industrial strategy is growing, the federal government does not yet have the people with the needed skill sets to generate and guide these policies.

Any public policy is only as good as its implementation, and the risks of getting industrial policy wrong are huge. These risks are heightened by the dearth of people who have the relevant expertise and experience. To rectify this, the United States needs to identify, support, and develop leaders who understand the economic context for these policies, have a sufficient background in the relevant science and technology, and possess the strategic mindset and skills to leverage that knowledge in developing and implementing successful policy.

To prepare for a future in which national industrial strategy is as integral as military preparedness, the federal government should launch an effort to recruit, train, and maintain a cohort of tech strategists operating across the government.

The Solution: A Tech Strategist Cohort

Developing a full cohort of leaders with all the required knowledge and skills will be a generational project. Carefully built multi-disciplinary teams will always be essential to meeting the country's needs. But the sooner that we start expanding the pool of well-rounded industrial strategists, the better. There are four actions that ought to be taken as soon as possible, ideally as part of a wider commitment to the future of U.S. industry.

First, the president needs to publicly embrace the need to identify and nurture a cohort of leaders who have knowledge of—and talent for—the disparate disciplines necessary to implement a national industrial strategy. There are three skill sets that these leaders must have. First, an understanding of the government's assets and authorities (such as labs, direct spending, tax incentives, contracting and acquisition, demonstration projects, regulation and deregulation) that can spur innovation. While this may suggest a turn to business executives or academics, the ability to run a company does not always translate into an appreciation of the complex interrelationship between government action, research, and market forces. Second, an appreciation for the new and emerging technologies that will define global power in the 21st century, and an understanding of the conditions required for the United States to grow the industries of the future and lead the new global markets that emerge. The United States likely should not pursue an industrial strategy focused on supporting national champions, but it will need to focus efforts on technologies key to national security and competitiveness; these leaders must have a meaningful understanding of which technologies are critical and how they are

[1] Ian Wallace, "One Thing Biden and Trump Seem to Agree On: We Need to Focus on Innovation," Slate, September 23, 2020.

developing. Third, strategic thinking. The United States will need leaders with the knowledge, skills, and experience to evaluate what is needed to build resilient supply chains given global markets and the ever-evolving plans of strategic rivals over the long term. This sort of strategic expertise is unique to government service and enhanced with years of experience, and therefore will be the hardest to acquire.

The second action that the president should take to advance the development of a cohort of tech strategists is designate an empowered leader with a small staff to grow this cohort and coordinate decisions with a small team operating from the National Security Council, the National Economic Council, and the Office of Science and Technology Policy.

Third, these capabilities will be needed throughout the government, not only in the Department of Commerce or the Department of Defense. The new office should identify and designate which government positions should be filled by cohort members and should work with the relevant departments and agencies to fill those positions. To ensure rapid and long-term impact, this staffing strategy should include pipeline development for junior positions as well as training and support for mid-career and senior leaders, such as providing economists with training in technology or instructing scientists in strategic thinking. In parallel, efforts should be made to enable the movement of cohort members in and out of government in ways that do not undermine ethical standards by using tools like special hiring authorities and pay flexibility. These efforts could dovetail with other ones to build new professional fields within government, such as the Cyberspace Solarium Commission's proposals to build cybersecurity capacity,[2] the U.S. Digital Service and 18F, which work to enhance the technical capabilities of federal agencies, and the proposals of the National Security Commission on Artificial Intelligence to build expertise in areas like artificial intelligence and quantum information science.[3]

Last, the office should seek funding to establish a national training capability—drawing on and adapting existing government assets—to provide a range of training and development opportunities for civil servants in emerging technologies, policy tools, and global markets. This training might leverage the expertise on strategic education within the professional military educational institutions. Other innovative models that have been introduced in recent years to attract and develop talent that the federal government lacks, like the designation of certain universities as Cyber Centers of Academic Excellence and the award of university scholarships through the CyberCorps, could be adapted to this purpose. And if a Digital Services Academy, as championed by the National Security Commission on Artificial Intelligence and modeled on the military service academies, is established, a Center for National Industrial Strategy could be established within it as a focal point of curriculum and best practice development. The ability to collect and use data and best practices will be key to this endeavor's success.

Conclusion

If the United States is to consider a national industrial strategy, it should be actively ensuring that its architects are well-qualified and trained in this critical area for U.S. leadership just as it invests in the strategic education of its generals and admirals.

[2] Cyberspace Solarium Commission, Growing a Stronger Federal Cyber Workforce, September 4, 2020.

[3] National Security Commission on Artificial Intelligence, 2020 Interim Report and Third Quarter Recommendations, October 2020.

November 2020

UPGRADING DIGITAL FINANCIAL INFRASTRUCTURE FOR FAIRNESS

KABIR KUMAR AND TILMAN EHRBECK

The Challenge: Dated Financial Infrastructure is Exacerbating Inequality

The shortcomings of the United States' retail financial systems became evident when the federal government responded to the economic fallout of the coronavirus pandemic. The payment system moved slowly: it took as long as three months to get payments to an estimated 100 million Americans, many of whom were facing sudden financial hardship.[1] In July 2020, months after many other countries had disbursed stimulus payments into bank accounts—often within minutes—millions had not yet received their prepaid cards.[2] In the absence of a national identity system, some payments were sent to deceased people, while fraudsters exploited state unemployment programs by using stolen identities.[3] Challenges also emerged with the credit-history-based credit-scoring system. The government mandated forbearance on loans, but the patchy application of forbearance codes in the existing credit system will likely make it harder to rebuild credit eligibility when people need it most.[4]

Even before the crisis exposed these shortcomings, the dated financial infrastructure in the United States was a driver of inequality.[5] Delays in getting paid push many individuals toward exploitative alternatives, such as small-dollar "payday" lenders or high-cost check cashers, which rake in $2 billion in fees every year; or they are left to face bank overdraft fees, which totaled $24 billion in 2016.[6] Prior to the crisis, an estimated 50 million Americans lacked sufficient credit histories to be scored by existing models, and another 80 million, many of them in minority households, paid higher prices or were denied financing because they had "non-prime" scores.[7]

The Solution: Upgrade the U.S. Digital Financial Infrastructure

The U.S. financial infrastructure needs to be upgraded for the digital age in three priority areas in order to make meaningful progress towards a fair system.

Instant Payments to Make Funds Available for Use Within Seconds

The United States needs a widely accessible instant-payment system where money sent from any bank account or digital wallet to another account or wallet is available for use within seconds. There are a number of ways to work toward this goal without wholesale changes to the underlying infrastructure. The Federal Reserve could extend the hours of operation of the instant automated clearing house system, the fastest retail payment system, as well as the underlying wholesale settlement system, Fedwire, to work around the clock.[8] Alternatively, Congress could amend the Electronic Funds Availability Act of 1987

[1] Aaron Klein, "How to fix the Covid stimulus payment problem: Accounts, information, and infrastructure," Brookings Institution, August 19, 2020.

[2] U.S. Government Accountablitiy Office, Coronavirus Oversight.

[3] Ibid.

[4] FinRegLab, Covid-19 Credit Reporting & Scoring Update, July 2020.

[5] Aaron Klein and George Selgin, "We shouldn't have to wait for FedNow to have faster payments," Brookings Institution, March 3, 2020.

[6] Theresa Schmall and Eva Wolkowitz, 2016 Financially Underserved Market Size Study, Center for Financial Services Innovation, November 2016.

[7] Unpublished mimeo, FinRegLab.

[8] Brookings Institution, How to make real-time payments real now, September 22, 2020.

to eliminate or dramatically reduce the two business days that banks can hold funds.

Ultimately, wholesale changes might be needed. The Federal Reserve could expedite FedNow, a new real-time payments system slated to go live in 2024, by incorporating existing private-sector platforms with the requirement that they be interoperable and compliant with network rules. This would avoid unnecessarily duplicating existing private-sector approaches. A similar instant-payment system in India, launched in 2016, now has an estimated volume 50 times that of the Federal Reserve's own instant automated clearing house, illustrating that a private-sector approach could achieve widespread instant payments faster.[9] These steps could get payments into people's pockets faster, reducing their reliance on predatory lenders and diminishing the prevalence of overdraft fees.

A System for Individuals and Businesses to Identify Themselves

The pandemic response in the United States has showed that the country needs a digital identity system that allows any individual or business to identify itself without compromising their privacy and security. Such a system can be implemented without universal biometrics or issuing a national ID card. A type of federated system could be built over time, leveraging existing data held by the government and the private sector, as has been done in Estonia.[10] Another contribution to this collection builds on the Estonian model to offer a proposal for a national digital identity system in the United States.[11] In Singapore, linkages among existing government datasets allowed pandemic stimulus payments to be distributed instantly.

As a first step, regulated financial services providers should be able to pull data on individuals from government agencies, such as the Internal Revenue Service (IRS), through secure application programmable interfaces (APIs). Congress has already required the IRS to begin building an income-verification API that could be part of an identification system based on government data; the creation of such interfaces should be expedited and expanded.[12] Ensuring the protection of sensitive personal financial data will be critical in such data-sharing schemes; another contribution to this collection offers a proposal for a cross-cutting federal privacy framework.[13] Additionally, federal regulators could facilitate the portability of "know your customer" (KYC) data between regulated financial providers to expedite the KYC process, as in Luxembourg.[14] These steps could realize some of the benefits of a national digital identity system in short order.

A Credit-Scoring System Based on Real-Time Data

The United States needs a credit-scoring system that operates in real time and relies on diverse sources of data. The existing system relies on historic credit usage and is likely to perpetuate inequities in lending.[15] This will make it harder for those most affected by the economic fallout of the pandemic to rebuild their lives with credit.[16] A new credit-scoring system needs to access better data and incorporate that data in models faster. For example, cash-flow data that reflects income and expenses is available for most consumers and businesses, and it can be captured in real time. Lever-

[9] Aaron Chaze, "India Sparks A Real-Time Payments Revolution," Global Finance, March 3, 2020.

[10] Economist, "Covid-19 strengthens the case for digital ID cards," September 5, 2020.

[11] Toomas Ilves, "Unlocking Digital Governance," in #Tech2021: Ideas for Digital Democracy.

[12] Peter Renton, "Congress Passes New Law to Mandate IRS Modernization," Lend Academy, June 17, 2019.

[13] Quentin Palfrey, "Advancing Digital Trust with Privacy Rules and Accountability," in #Tech2021: Ideas for Digital Democracy.

[14] Jamie Leee, "MAS to reboot e-KYC project," Business Times, November 13, 2019.

[15] Caroline Ratcliffe and Steven Brown, "Credit scores perpetuate racial disparities, even in America's most prosperous cities," Urban Institute, November 20, 2017.

[16] FinRegLab, Covid-19 Credit Reporting & Scoring Update, July 2020.

aging such data has substantial promise for inclusion and fair lending.[17]

Use of this data for new lending models could be scaled system-wide if existing models are adjusted and better data secured. Financial regulators have signaled increasing openness to allowing the use of cash-flow data in credit underwriting.[18] But they also need to encourage faster adoption. It took over five years after the last financial crisis for lenders to update their models and even today the most widely used models use pre-2008 data. Regulators and Congress should provide greater clarity to lenders about validation and compliance expectations, reduce lenders' barriers to data, and strengthen consumer protections.[19]

Conclusion

These digital infrastructure upgrades are based on financial data flows in the digital age. The United States needs a modern framework for finance that updates rules for accessing, controlling, moving, and utilizing data. Congress can act on multiple fronts. Immediately, it can encourage the Consumer Financial Protection Bureau to enable financial data portability under the authority it was given in the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[20] In the medium term, Congress needs to upgrade laws on privacy and control in finance, such as the Financial Modernization Act of 1999.[21] By modernizing the infrastructure of the financial system, the United States can address inequalities, remove inefficiencies, and make its financial system fit for the digital age.

[17] FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings, July 2019.

[18] Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, "Interagency Statement on the Use of Alternative Data in Credit Underwriting," December 3, 2019.

[19] FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Market Context & Policy Analysis, February 2020.

[20] Consumer Financial Protection Bureau, "CFPB Announces Plan to Issue ANPR on Consumer-Authorized Access to Financial Data," July 24, 2020.

[21] Unpublished mimeo, Financial Health Network.

November 2020

REFORMING THE PATENT SYSTEM TO SUPPORT INNOVATION

LISA LARRIMORE OUELLETTE AND HEIDI WILLIAMS

The Challenge: Stagnating Productivity Growth

In recent decades, economic growth has slowed in the United States, largely due to a slowdown in total factor productivity growth—the portion of growth not explained by the traditional inputs of capital and labor.[1] Even before the coronavirus pandemic, the Congressional Budget Office projected this trend to continue in the coming years. Economists generally agree that the only way to secure long-run productivity growth in the United States is through innovation. Hence, a key challenge facing policymakers is how best to design policies to accelerate innovation.

The patent system is one policy lever designed to do this. Its basic logic is simple. By allowing inventors to capture a higher share of the social value of their inventions than they would in a competitive market, the system aims to encourage the development and disclosure of new ideas. But these benefits come with costs: the patent system has been criticized for imposing not only higher prices on patented goods purchased by consumers, but also for potentially discouraging subsequent inventors.

In the past several decades, there has been growing concern about the costs imposed by patents, especially those stemming from frivolous litigation. Unfortunately, there is little credible evidence of whether such costs are outweighed by the benefits of the patent system. Consequently, debates on reform tend to be based on ideologies and theories rather than data and evidence. However, despite this lack of evidence, the design of the patent system can be improved. Two proposed reforms could create a more favorable framework for innovation even without resolving broader questions about the costs and benefits of patent protection. They are clearer labeling of prophetic examples and increased transparency in patent ownership.

The Solution: Innovation-Friendly Reforms to the Patent System

Labeling Prophetic Examples

The first proposed reform focuses on the common practice of patent applicants including hypothetical experimental methods and results—known as prophetic examples—in their patent applications. A key goal of the patent system is for accurate information about new inventions to be disclosed to the public. Patent-induced disclosures are intended to serve a teaching function, facilitating spillovers of the technical knowledge embodied in patents to others. Specifically, the Patent Act requires that patent applicants describe their invention at a sufficient level of detail that an individual skilled in the relevant technological area could make and use the invention ("enablement"), and could recognize that the inventor possessed the invention ("written description"). To satisfy these disclosure requirements, inventors often include working examples summarizing data and previously conducted experiments. Although not widely known—even among individuals who closely study the patent system—patent applications also often include prophetic examples. Unlike working examples, prophetic examples report experiments, procedures, and protocols that have not actually been conducted. Instead, inventors predict or "prophesize" the results

[1] This brief draws from Lisa Larrimore Ouellette and Heidi Williams, "Reforming the Patent System," Hamilton Project Policy Proposal 2020-12, June 2020.

of an experiment. Although perhaps surprising, both the U.S. Patent and Trademark Office (USPTO) and federal courts agree that prophetic examples satisfy all disclosure requirements of the Patent Act.

In theory, prophetic and working examples can be distinguished by reading the verb tense: working examples are presented in the past tense, whereas examples in the present or future tense are likely prophetic. However, this rule is not well understood by many market participants.[2] Recent research documents two key pieces of evidence that together suggest that prophetic examples are a problem in practice.[3] First, prophetic examples are common: 17 percent of examples in a recent set of U.S. biology and chemistry patents are prophetic, and of the patents with examples in that sample at least 24 percent contain some prophetic examples. Second, the potential costs of prophetic examples appear to be large: of 100 randomly selected patents that use only prophetic examples and are cited in a scientific publication for a specific proposition, 99 are cited in a way that—incorrectly—treats the prophetic example as a real example, such as by saying that an experiment "had been carried out" by authors of the cited patent.

There is a straightforward case for requiring that prophetic examples be more clearly labeled. The only cost would be lost benefits to patentees that are generated by creating misunderstandings among market participants, which is not a net social benefit. In terms of regulatory burden, patent applicants are already asked to distinguish between prophetic and working examples in their written tenses, so adding a clear label is not a heavy burden. This reform is firmly within the USPTO's authority to implement, or the change could also be made at the direction of Congress.

Increasing Transparency in Patent Ownership

The second proposed reform addresses the failure of the system to provide accurate notification about who owns patents. Currently, the first page of a patent lists the assignee as reported by the applicant at the time the application is granted. Any subsequent changes in assignment can be voluntarily recorded with the USPTO, but there is no legal requirement for patentees to publicly record changes in ownership.[4] On a more practical level, there is no standardized process for recording the names of patent owners, implying that any given owner is often referred to by different names in different patents. A more complicated issue is that so-called hidden owners—such as ultimate parent entities or owners who use shell companies to shield their identities—are not listed in current records (which include only titleholders). These problems likely increase transaction costs throughout the patent system.

The USPTO attempted to address these problems in 2014 but the proposed regulation was abandoned primarily because its focus on hidden owners led to concerns from patent holders about increased regulatory costs. A more tailored set of reforms would avoid such controversy. First, for all patents, linking patent records to unique IDs and requiring titleholders to update ownership records regularly would reduce the administrative and transaction costs of the system with relatively little burden for patentees. Second, for patents asserted in litigation, requiring disclosure of hidden owners would facilitate settlement and limit litigation abuse.

Conclusion

A robust patent system is a key component of any innovative economy and improving that system can support innovators across sectors. In contrast with traditional patent-reform debates, which can be easily derailed by ideological issues, the two more tailored reforms proposed here are easier to justify based on existing theory and evidence. These reforms should be enacted so as to spur innovation and help counteract declining productivity growth in the United States.

[2] Janet Freilich and Lisa Larrimore Ouellette, "Science Fiction: Fictitious Experiments in Patents," Science 364:6445, June 14, 2019.

[3] Janet Freilich, "Prophetic Patents," U.C. Davis Law Review, 2019.

[4] U.S. Patent and Trademark Office (USPTO),"Changes to Require Identification of Attributable Owner," Federal Register 79 (16), January 24, 2014.

November 2020

AVERTING A CRISIS OF CONFIDENCE IN ARTIFICIAL INTELLIGENCE

R. DAVID EDELMAN

The Challenge: An AI Revolution, Derailed

The devices and systems in our lives are being slowly infused with artificial intelligence (AI) technologies driven by machine learning. Some deliver delights, like smarter cameras in our phones that turn casual clicks into works of art. Others breed more ambivalence, like ads in your newsfeed showing precisely what you needed to buy this week; convenient, yes, but to some, invasively prescient.

But more socially significant applications of AI are getting far less attention, despite representing the greatest risk and opportunity for that technology in the coming decade. They include systems that can convince a bank to extend a loan to an under-served borrower with a thin credit file, or that can have a human-like conversation with a refugee to help them navigate byzantine asylum bureaucracies. But they also include facial-recognition systems that are partially blind to large swathes of the population, with plunging performance when presented with female or black faces, and AI-driven employment systems that silently deny opportunity to those who do not live near or sound like those already successful at the same job.

AI technologies are still in their infancy—with immense potential, largely untapped, but also with fundamental usability questions still unclear. The performance of these systems varies wildly: AI systems that excel at one complex task might fail spectacularly at another that is, to human minds, adjacent. Many of the most powerful systems have little to no ability to explain themselves. They are only as accurate as the data they are trained upon, and even then, performance against edge cases is often imperfect. In short, AI systems are constantly surprising researchers in what they can do and what they fail to do—and that raises significant implications for public policy.

As societies, we have learned to be tolerant of computer failure in our lives: a dropped call here, a few minutes of lost writing there. When socially significant systems let us down, though, they do not just take something from the user; they take something from society. They erode trust in the systems used by our government, and thus in the government itself. They antagonize the very communities that the police most need to partner with to tackle crime. They do not just hold back opportunity in ways that cause social and economic stagnation—they may well be illegal.

AI systems deployed in socially significant areas before the technology is ready may lead us to skepticism of their capabilities: a crisis of confidence in AI with implications far beyond technology—for economic dynamism, social justice, education, and more. Fixing this skepticism will not just be a matter of filing a bug report. Blame will lie not just with the programmers but with public officials and will carry public consequences. So the challenge of the next few years is to get ahead of this crisis and show that it is within the power of governments, with the right insights, to apply the tools of public policy to check the harms of misbehaving AI—and in so doing to coax into existence a friendlier, more reliable breed of machine.

The Solution: To Govern AI, Evolve from Principles to Practice

Governments around the world are rushing to demonstrate they have a handle on the social and economic complexity—and opportunities—of AI. There are innumerable new commissions, study groups, task forces and high-level statements, especially on both sides of the Atlantic. So, what should the aim of all these efforts on such a new, general-purpose technology be—particularly when AI's true significance in our daily lives has yet to be seen?

If all the governmental projects to govern AI to date can be summed up in a single word, it would be: "principles." From the European Commission to the U.S. Defense Department, Google to Microsoft, the OECD to the G20, high-level statements of principles abound. Most have an explicitly ethical orientation, a conscious counterpoise to a decade in which many declared technological systems "neutral by design," leaving democracies to pick up the pieces of their ill-design. And many have substantial overlap, highlighting the importance of privacy, accountability, and—with slightly weaker consensus—transparency and human control. Many represent careful consideration of the harms of AI run amok. Yet few if any purport to offer solutions, particularly in the real world of public policy, where even the simplest decision comes with tradeoffs.

This is where the opportunity lies to avert the crisis of confidence in AI; to match the ambition and ethical orientation of these principles with the hard, exacting, and context-specific work of policymaking. The first step is recognizing that most governments will not have a singular "AI policy" any more than they can have one "computing policy"—the concept is so broad as to be meaningless. Rather, the last 30 years have given rise to a diversity of laws governing computer-enabled conduct, like balancing rightsholders' interests and fair-use principles, or defining crimes like "intrusion" in the digital space and limiting governments' ability to access private data and networks. Over these same three decades, policymakers have gradually developed an instinct to know when digital systems can be trusted to support human judgment and when they are best left out of the decision-making process.

The challenge for this era of AI is to do both, again: to develop the detailed policies that allow us to contextualize AI systems and govern them accordingly, and to develop the "gut sense" of their readiness to play more significant roles in our lives.

The first step is for the regulators of banks and lending, medicine, employment, and other key sectors to understand how AI systems are being used; to visualize the consequences of systems of limited (or exceptional) performance; and to adapt their regulations and enforcement to confront those very real harms. The threshold of acceptable transparency is bound to differ in seeking the reasons for a loan rejection as compared to a parole denial. The method to prove the performance of a safe cargo drone will certainly differ from proving a hiring system does not discriminate. The immediate task for government is to determine how precisely to apply long-standing protections to this new technology—and, where necessary, establish the parameters of policy-aware design so that those building systems understand what is required to build with equity and accountability in mind. A government with a national AI strategy is one that can point to all of its obligations—especially responsibilities to protect—and explain how it is applying the principles that animate laws to the uses of AI, built atop technical expertise in agencies buttressed by appropriate regulation.

Conclusion

After this hard, unglamourous, crucial work has completed its first stages, themes will undoubtedly emerge. They may well reflect some of those high-level principles of the last few years. More likely, gnarled by contact with policy realities, they will be more recognizable as best practices, common regulatory frameworks, or even shared datasets and evaluation mechanisms for the use of AI in socially significant systems. Here there is immense potential, particularly between the United States and Europe, to develop a commonality in the evaluation of systems necessary for common markets. It is harder to arrive at common safety standards for vehicles than it is to talk about our shared commitment to protect passengers. But governments have managed to do both before and they have the opportunity to do so now with socially siginifcant AI systems—before the full extent of envisaged harm has come to pass.

November 2020

PROTECTING DEMOCRACY AND PUBLIC HEALTH FROM ONLINE DISINFORMATION

KAREN KORNBLUH

The Challenge: Disinformation Undermines our Ability to Govern Ourselves

In July, a video entitled "America's frontline doctors" was a runaway train racing across the major digital platforms. The video hosted on Breitbart's Facebook page claimed that face masks are dangerous, social distancing is unnecessary, and the drug hydroxychloroquine is a miracle cure for the coronavirus. It racked up 20 million views in just 12 hours on Facebook alone, before it was ultimately removed by Facebook, Twitter, and YouTube for violating their guidelines.

Today only about half of Americans say they would take a coronavirus vaccine when it is available—not enough to provide for herd immunity.[1] According to one poll, over 40 percent of Americans would decline a shot in part because they believe the vaccine is a scheme by Bill Gates to implant a microchip inside them.[2]

The platforms deserve credit for limiting some of the disinformation related to the U.S. presidential election count but hoaxes continued to spread through private groups, such as QAnon, which now has millions of adherents.[3] A report by the campaigning network Avaaz reveals that health misinformation generated a staggering 3.8 billion views on Facebook globally in the past year.[4] GMF Digital has found that websites that repeatedly publish false content or that gather and present information irresponsibly have increased their interactions on Facebook in the United States threefold since early 2017, and they now rival some of the most reputable news outlets.[5]

Relying on platforms to play whack-a-mole with individual pieces of dishonest content is clearly not working. In fact, the number of posts that would require whacking is so vast that any platform with the power to monitor it all in real time would itself represent a further threat to the democratic tenet of free speech.

But the disinformation emanates from an ecosystem of manipulation that the platforms could disable with sufficient commitment. A relatively small number of high-traffic outlets launder content as news: the top ten of GMF Digital's most engaged-with deceptive sites are responsible for 62 percent of the interactions among 721 sites in the sample. The content from these outlets is promoted by networks of pages, influencers, and groups and then algorithmically promoted to many more users through their newsfeed.

Despite all the new anti-disinformation rules announced by platforms, the manipulation ecosystem continues to operate online, enlisting users into inadvertently spreading disinformation to others. An Internet utopianism characterized by the belief that the network would enhance democracy by its very design—bringing voice to the voiceless, power to the powerless, and the wisdom of crowds—lulled many

[1] Ben Kamisar and Melissa Holzberg, "Poll: Less than Half of Americans Say They [Will] Get a Coronavirus Vaccine," NBC News, August 18, 2020.

[2] Andrew Romano, "New Yahoo News/YouGov Poll Shows Coronavirus Conspiracy Theories Spreading on the Right may Hamper Vaccine Efforts," Yahoo News, May 22, 2020.

[3] Ari Sen and Brandy Zadrozny, "QAnon Groups have Millions of Members on Facebook, Documents Show," NBC News, August 10, 2020.

[4] Avaaz, Facebook's Algorithm: A Major Threat to Public Health, August 19, 2020.

[5] Karen Kornbluh, Adrienne Goldstein, and Eli Weiner, New Study by Digital New Deal Finds Engagement with Deceptive Outlets Higher on Facebook Today Than Run-up to 2016 Election, German Marshall Fund of the United States, October 12, 2020.

into assuming it should be a policy-free zone. But, as our lives and our news consumption moved online, the Wild West atmosphere created too many opportunities for malign actors to manipulate users, distort democratic debate, and undermine the consensus building needed to address major challenges like the one the coronavirus presents.

The Solution: Change the Incentives to Protect the Digital Public Square

Dismantling the disinformation ecosystem, as GMF Digital proposed in its roadmap for Safeguarding Digital Democracy, must avoid conscripting government or industry to play the role of "truth police."[6] Instead, platform incentives should be changed so that expectations for fairness from the analog world would be honored in the digital world. For this new system to work, platforms should implement a new circuit breaker system to give them time to act. And a new Public Broadcasting Service (PBS) of the Internet should be created to support independent journalism.

Updating expectations from the analog world for the digital era would start with campaign advertising transparency as required by the proposed bipartisan Honest Ads Act.[7] Consumers should be protected against computer-generated deceptions such as deepfakes and the intrusive collection and use of their personal data—just as they are protected against fraud offline. Civil rights protections against discrimination and harassment must apply online as well. Importing a version of the transparency that offline journalism traditionally practices (for example, through bylines and mastheads) would hold platforms accountable to the public for enforcing their own rules, such as limiting the reach of websites that repeatedly violate platform standards. It would also help users protect themselves against manipulation by clarifying the origins, coordination, and funding sources for websites, pages, channels, influencers, and groups.

These new practices can only be put in place if the lightning speed of online information sharing can be paused before it does irreversible harm. Platforms should employ "circuit breakers"—like those used to prevent market-driven panics and slow down high-frequency trading—to halt the viral rollercoaster and give platforms the opportunity to evaluate content before it reaches a mass audience.[8] Intervention by a human able to determine if a piece of content violates platform guidelines would ensure that platforms are aware of dangerous viral spread as it happens, rather than after the damage has been done. Twitter and Facebook have said they are already considering variations on this notion.[9]

Finally, users need sources of accurate information. As the advertising revenues that once supported independent journalism have moved to the platforms, it has become clear that journalism is a public good in need of support. A PBS of the Internet would have platforms that subsidize the news content from which they—and democracy—benefit.[10]

Conclusion

It has become clear that the current whack-a-mole approach to disinformation is inadequate. At a time of a public-health emergency and democratic erosion, the information ecosystem can be cleaned up by updating analogue expectations of fairness for the digital world, including transparency about rules and sources of information, and treating independent journalism like the public good that it is.

[6] Karen Kornbluh and Ellen P. Goodman, Safeguarding Digital Democracy, German Marshall Fund of the United States, March 24, 2020.

[7] Senate, Honest Ads Act (S. 1356), introduced on May 7, 2019.

[8] Ellen P. Goodman and Karen Kornbluh, "Social Media Platforms Need to Flatten the Curve of Dangerous Misinformation," Slate, August 21, 2020.

[9] See Vijaya Gadde and Kayvon Beykpour, Additional Steps We [are] Taking Ahead of the 2020 U..S Election, Twitter, October 9, 2020; and Hamza Shaban, "WhatsApp is Trying to Clamp Down on Viral Misinformation with a Messaging Limit," Washington Post, January 22, 2019.

[10] Ellen Goodman, "Building Civic Infrastructure for the 21st Century," in #Tech2021: Ideas for Digital Democracy.

CONTRIBUTORS

Adam Bobrow is the founder and CEO of Foresight Resilience Strategies and a senior fellow with GMF Digital. He previously served as the senior policy advisor for international affairs in the White House Office of Science and Technology Policy.

Edward Cardon is a senior counselor at the Cohen Group. He previously served as head of Army Cyber Command.

Sam duPont is the deputy director of GMF Digital. He previously served as director for digital trade at the Office of the United States Trade Representative.

R. David Edelman is based at MIT's Internet Policy Research Initiative, where he holds joint appointments at the Computer Science & AI Lab (CSAIL) and Center for International Studies (CIS) and teaches in the Department of Electrical Engineering and Computer Science. He previously served at the State Department and White House, most recently as special assistant to President Obama for economic & technology policy.

Tilman Ehrbeck is a managing partner at Flourish Ventures and serves as chair of the Advisory Council to the U.N. Special Advocate for Inclusive Finance in Development.

Ellen P. Goodman is a professor at Rutgers Law School, the co-director and co-founder of the Rutgers Institute for Information Policy & Law, and a senior fellow with GMF Digital.

Thomas Hedberg is an associate research engineer with the Applied Research Laboratory for Intelligence and Security at the University of Maryland.

Reed Hundt is the founder and CEO of the Coalition for Green Capital. He previously served as chairman of the Federal Communications Commission.

Will Hurd represents Texas' 23rd Congressional District in the U.S. House of Representatives. He serves on the board of directors of the German Marshall Fund of the United States.

Toomas Ilves is a distinguished visiting fellow at the Hoover Institution at Stanford University. He previously served as President of the Republic of Estonia.

Karen Kornbluh is a senior fellow and director of GMF Digital. She previously served as the U.S. Ambassador to the Organization for Economic Cooperation and Development and as a senior official at the Federal Communications Commission and the U.S. Department of Treasury.

Kabir Kumar is a director at Flourish Ventures.

Lara Mangravite is the president of Sage Bionetworks.

Lisa Larrimore Ouellette is a professor of law and Justin M. Roach, Jr. Faculty Scholar at Stanford Law School.

Quentin Palfrey is the president of the International Digital Accountability Council and a senior fellow with GMF Digital. He previously served in the White House Office of Science & Technology Policy and at the U.S. Department of Commerce.

Rashida Richardson is a visiting scholar at Rutgers Law School and the Rutgers Institute for Information Policy & Law, and a senior fellow with GMF Digital.

Harvey Rishikof is director of Policy and Cyber Security Research at the Applied Research Laboratory for Intelligence and Security at the University of Maryland. He previously served as senior policy advisor to the director of national counterintelligence at the Office of the Director of National Intelligence.

Christopher Schroeder is the co-founder and general partner of Next Billion Ventures and is a serial entrepreneur, advisor, and investor in interactive technologies around the globe. He serves on the board of directors of the German Marshall Fund of the United States.

Laura Taylor-Kale previously served as deputy assistant secretary for manufacturing at the U.S. Department of Commerce. She is the co-author of The Work Ahead: Machines, Skills and U.S. Leadership in the Twenty-First Century.

Ian Wallace is a senior fellow with GMF Digital and chair of the Strategy & Policy Working Group of the Global Forum on Cyber Expertise.

John Wilbanks is the chief commons officer at Sage Bionetworks.

Heidi Williams is the Charles R. Schwab Professor of Economics at Stanford University, a senior fellow at the Stanford Institute for Economic Policy Research, and a research associate at the National Bureau of Economic Research.

November 2020

The views expressed in GMF publications and commentary are the views of the author(s) alone.

About GMF Digital

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) works to support democracy in the digital age. GMF Digital leverages a transatlantic network of senior fellows to develop and advance strategic reforms that foster innovation, create opportunity, and advance an equitable society.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org