

The Berggruen Institute

RENOVATING DEMOCRACY FOR THE DIGITAL AGE

Emerging Solutions Framework
August 2017

PROJECT TEAM

Matt Browne, Founder, Global Progress, Founder

Dawn Nakagawa, Executive Vice President, Berggruen Institute

Ariel Ratner, Founder & CEO, Inside Revolution

Jody Sadornas, Program Manager, Berggruen Institute

Ola Tjornbo, Principal, Achipelago Consultants

CONTENTS

Executive Summary.....	3
Renovating Democracy: The Challenge.....	5
Promising Solutions.....	8
Protecting the Integrity of the Democratic Process.....	9
An Alliance against Digital Threats to Democracy aka “Cyber NATO”	9
Technology Industry Standards Group.....	10
Rebuilding the Public Square.....	13
Aligning Incentives for Pro-Democratic Social Media.....	14
A Viable Fourth Estate.....	15
Digital Literacy.....	16
Innovating for More Effective Governance.....	18
Redesigning Democratic Institutions.....	18
Charismatic Transparency.....	21
Conclusion: Renovating Democracy for the Digital Age	23
Glossary.....	24
Notes.....	25
Appendix.....	28

EXECUTIVE SUMMARY

The advent of the Digital Age was imagined to be the signature development in the advancement of democracy worldwide. Information and communications technologies (ICTs), in this view, were to provide greater access to knowledge and more avenues for connecting and engaging with each other, and indeed they have. Nevertheless, the downsides and discontentment of the Digital Era had also become increasingly apparent. Broader trends, like the proliferation of misinformation and political polarization, among other consequences, while not solely caused by digital technologies, seem to be exacerbated by their development.

Just as leaders and citizens responded to the challenges of the Industrial Era with new “solutions” for democracy, so too must leaders and citizens respond to the Digital Era with a new “solution set” for democracy now. Over the past year, the Berggruen Institute’s Renovating Democracy for the Digital Age project team has undertaken to identify potential solutions. Through initial conversations with technologists, policy makers, and academics, the team has identified a set of ideas for strengthening democracy and rebuilding the public square. We have divided these solutions into three areas, including:

- 1 PROTECTING THE INTEGRITY OF THE DEMOCRATIC PROCESS:** These solutions focus on protecting our electoral systems against the real and immediate threats they face in the form of hacking and fake news, which are undermining the legitimacy of government.
- 2 REBUILDING THE PUBLIC SQUARE:** These solutions address the damage that has been done to the information ecosystem. We need to both strengthen the traditional fourth estate, and to find ways to adapt the new social media platforms that have entered into this landscape so that they support, rather than hinder, civic deliberation.
- 3 INNOVATING FOR MORE EFFECTIVE GOVERNANCE:** These solutions tackle the long term negative trends of declining trust and increasing political polarization that are afflicting many modern democracies. We believe this needs to be done by reforming our governance systems so that the institutions reduce rather than amplify the civic disruption, and find new ways to engage citizens in the process of government.

The solution set presented here, at the mid-point of the project, should not be considered a final set of recommendations, but ideas for further consideration and development. As a second phase to this endeavor, the Berggruen Institute will expand the geographic bounds of this exploration to gather feedback from constituents of other democracies while also focusing on further developing a few of the more promising ideas.

RENOVATING DEMOCRACY: THE CHALLENGE

Less than a decade after the Global Financial Crisis undermined confidence in our economies, a no less epoch-making political crisis is now shaking democracies worldwide. As the 21st century unfolds, technology and globalization are not only transforming our economies, but also our institutions of government and the broader public square.

Initially, many heralded the advent and proliferation of communication technology as a new dawn for democracy and prosperity. Indeed, the information age presents new opportunities for economic growth, enhanced health and security, and more effective governance.¹ Equally, our democratic institutions have leveraged new tools to enhance civic and political participation, democratize access to information, and address intractable public policy challenges.² However, more recently—and quite intensely since late 2015—our information and communication technology landscape has posed challenges and exposed new vulnerabilities to our democratic institutions.

The digital age has brought with it cyber security threats that were initially confined to cyber espionage, IP theft, and cyber vandalism. More recently, it has provided a new array of tools for nefarious forces looking to disrupt democratic norms and undermine stable governance.³

There is mounting evidence that communication technology, and social media in particular, has the effect of deepening political polarization and social fragmentation.⁴ The attention economy relies on generating audiences. This is best achieved by telling people what they already believe and doing so in a way that elicits emotion. Confirmation bias and political outrage within virtual forums of the like-minded create a steady flow of traffic, rewarding extreme views and vitriol at the expense of civil deliberation—and too frequently, the truth.

Lies, mischaracterization, and bias interpretation are not new problems in politics, but the speed and distance with which social media allows them to travel is unprecedented, making it an outsized threat to the development of the well-informed citizens that democracy requires. Unhindered by the costs associated with producing quality news, fake news sources easily proliferate and, precisely because such content is designed to be entertaining without the constraint of truth, are more viral. Citizens become unwitting participants in the spread of “fake news” falling prey to stories that support their narrative about political adversaries.⁵ As one study showed, during the 2016 U.S. presidential elections, fake news stories were

¹ For further description and discussion on the promise of Big Data and the Information Age, see <http://23.66.85.199/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf>.

² For further description and discussion on the challenges of Big Data and the Information Age, see <http://23.66.85.199/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf>.

³ For further description and discussion on the challenges to our democracies brought on by ICTs and social media, see http://www.pakistansocietyofcriminology.com/publications/2012_08_10_4110.pdf#page=117.

⁴ For further description and discussion on how social media creates social instability, see <http://knowledge.wharton.upenn.edu/article/how-social-media-leads-to-a-less-stable-world/>.

⁵ Lenarz, Julie. “Russia Has Made Fake News Into A Weapon That Threatens Democracy in Europe.” *The Telegraph*. 26 Jan 2017, <http://www.telegraph.co.uk/news/2017/01/26/russia-has-made-fake-news-weapon-threatens-democracy-europe/>.

shared on Facebook 8.7 million times while real news was shared 7.3 million times.⁶ Similarly, in the months leading up to the 2016 election, the amount of engagement on social media for posts from sites such as Freedom Daily, on which almost half the content is false or misleading, was on average nearly 19 times higher than for posts from mainstream news outlets.⁷

“Lies, mischaracterization, and bias interpretation are not new problems in politics, but the speed and distance with which social media allows them to travel is unprecedented, making it an outsized threat to the development of the well-informed citizens that democracy requires.”

Fake news has led to the collapse of broadly shared public narratives and in some cases even shared facts. It has also further undermined confidence in the reliability of the news media, which in turn is part of the broader crisis of faith in expertise. Digital technologies have lowered barriers to entry creating an explosion in new sources for news. To compete, traditional media that formerly played the role of gatekeepers, in principle responsible for quality assurance, have tended toward more extreme positions, generally defined along partisan lines to draw audiences. This has pulled audiences and reporting capacity apart and led to a fragmentation of the news audience.^{8,9} In this new media

landscape, politicians and journalists alike are free to denounce unwelcome information as politically motivated ‘fake news’, with no authoritative arbiter to sort truth from falsehood.

Additionally, the digitization of the public commons has moved political discourse online and brought with it the normative incivility of the space. Simply put, people are willing to say things online—in comment threads, on Twitter, on Facebook—that they would never say to someone’s face, and this is even more true when people are able to make their comments anonymously. The decline of civil discourse is aggravated by the enhancement of echo-chambers that reward extreme positions and polarize the population. The list of consequences and vulnerabilities reverberating through democracies continues to grow.

The impact on government from these forces is particularly concerning. Unable to keep pace with technological innovation and deployment—neither in its adoption nor in its regulation—

⁶ Silverman, Craig. “This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook.” *Buzzfeed*. 16 Nov. 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.khXXlenYO#.abvLE29j8. Accessed 28 Aug 2017.

⁷ Bell, Emily and Taylor Owen. “The Platform Press: How Silicon Valley Re-engineered Journalism.” *Tow Center for Digital Journalism*. 29 March 2016, www.cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php Accessed on 26 April 2017.

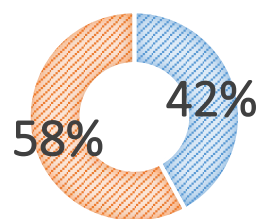
⁸ Sunstein, Cass. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press, 2017.

⁹ The Pew Research Centre reports that 44% of Americans now get news on Facebook (Gottfried, Jeffrey and Elisa Shearer. “News use Across Social Media Platforms 2016.” *Pew Research Center*. 26 May 2016, <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>. Accessed on 26 April 2017.). That, combined with a decline in the traditional press corps (“Today’s Washington Press Corps More Digital, Specialized.” *Pew Research Center*. 3 Dec 2015, <http://www.journalism.org/2015/12/03/todays-washington-press-corps-more-digital-specialized/>. Accessed on 26 April 2017.), some argue, are exacerbating political polarization (Gandour, Ricardo. “Study: Decline of traditional media feeds polarization.” *Columbia Journal Review*. 19 Sep 2016, https://www.cjr.org/analysis/media_polarization_journalism.php. Accessed on 26 April 2017.). For further description and discussion, see also <https://www.brandwatch.com/blog/react-the-prevalence-of-fake-news-and-why-we-are-more-misinformed-than-ever/>.

and unable to protect itself from hacks that expose state secrets and private emails, governments appear ineffective and incompetent, accelerating a decades-long trend of declining trust in political elites.¹⁰ Additionally, politicians are not immune from the conditioning of a polarized society that expects them to adhere unwaveringly with partisan positions. Compromise becomes impossible when shaking hands with those across the aisle is perceived as fraternizing with the enemy.

GLOBAL TRUST IN GOVERNMENT

■ Trust in Government ■ No Trust in Government



As traditional parties fail to live up to promises to protect citizens from the forces of technology and globalization, citizens are increasingly looking to political outsiders. Some of these outsiders offer genuine alternatives and are seeking to equip society to meet its political and economic challenges, but others are demagogues looking to profit from fear and pessimism created by this uncontrolled change.¹¹ We have seen early signs that these developments now threaten some of the recent achievements of liberal

democracy as countries begin to turn their backs on open borders, trade, and closer political integration. Brexit, the rise of far-right candidates and parties across Europe, and the 2016 U.S. presidential election: all are evidence of more divided, more fearful, and less optimistic societies.

Information technology is not the only nor necessarily the immediate cause of all these trends, many of which stretch back to before the widespread availability of the Internet and social media. However, it is now clear that communication technology is aggravating and accelerating these problems and giving new tools to those who would use them to divide and destabilize democracy.¹² Indeed, evidence points to the number of ways in which social media contributes to making us less tolerant, more fearful, more distrustful, and more vulnerable.

At a minimum, these effects undercut the ability of society and politicians to work together to solve policy issues. At worst, they call into question the legitimacy of a democratically elected government.

Democracies across the world must take seriously the need to adapt government and society to the digital age. Governments, civil society, tech companies, and the public must work together to defend and protect our democratic institutions and defend the values upon which they are founded. This undertaking requires a great deal of political will, courageous

¹⁰ The Organization for Economic Co-operation and Development (OECD) reports that in 2017, on average, only 42% of OECD citizens had trust in their national governments continuing a long term declining trend (OECD. "Government at a Glance 2017." *OECD Publishing*. 2017, http://dx.doi.org/10.1787/gov_glance-2017-en).

¹¹ According to Ipsos Global Trends, globally in mature economies, people are pessimistic about the future of their country (Page, Ben. "This Way Up." *Ipsos Global Trends*. 2017, <https://www.ipsosglobaltrends.com/this-way-up/>. Accessed on 26 Aug 2017.).

¹² For further description and discussion on how communication technology is creating division and instability in democracies, see <http://www.tandfonline.com/doi/abs/10.1080/13510340008403642?journalCode=fdem20>.

leadership and human ingenuity to resolve. New ideas for how to overcome polarization, revitalize quality journalism, and restore public trust in government must be developed and implemented.

PROMISING SOLUTIONS

The emerging solution set outlined in this paper is based on a year-long exploration by the Berggruen Institute’s project team on Renovating Democracy for the Digital Age which hosted roundtable discussions in Montreal, New York, Lisbon, Menlo Park, and Washington, D.C.¹³ These discussions have included technologists, politicians, activists, journalists, and academics, each providing their perspective on the challenges digital technologies pose to democracy, and presenting possible ways to address them. The ideas contained in here are neither exhaustive nor final. At this, the mid-point in the project, we seek only to present a number of possible solutions for consideration and further development.

Renovating democracy will require a lengthy process involving meeting immediate threats, strengthening our fundamental democratic institutions, and innovating in order to meet the challenges of the future. Towards that end, we have divided our preliminary solutions into three categories:

- 1 **PROTECTING THE INTEGRITY OF THE DEMOCRATIC PROCESS:** These solutions focus on protecting our electoral systems against the real and immediate threats they face in the form of hacking and fake news, which are undermining the legitimacy of government.
- 2 **REBUILDING THE PUBLIC SQUARE:** These solutions address the damage that has been done to the information ecosystem. We need to both strengthen the traditional fourth estate, and to find ways to adapt the new social media platforms that have entered into this landscape so that they support, rather than hinder, civic deliberation.
- 3 **INNOVATING FOR MORE EFFECTIVE GOVERNANCE:** These solutions tackle the long term negative trends of declining trust and increasing political polarization that are afflicting many modern democracies. We believe this needs to be done by reforming our governance systems so that the institutions reduce rather than amplify the civic disruption, and find new ways to engage citizens in the process of government.

¹³ For a complete participation list, see Appendix F.

1. PROTECTING THE INTEGRITY OF THE DEMOCRATIC PROCESS

The integrity of the democratic process is under threat from cyberattacks, both from within and without. Toomas Ilves, the former President of Estonia and current senior fellow at the Hoover Institute at Stanford University, has outlined six distinct attack vectors that cyber operatives can use to disrupt the integrity of the democratic process:

ATTACKS ON VOTER REGISTRATION LISTS

Either for voter suppression or to harvest information for targeted political messages

HACKING

Of email servers to steal private information held by political parties

DOXING

The publishing of compromising private information timed to disrupt political campaigns

FAKE NEWS

Misleading news and propaganda that is disseminated in order to undermine electoral processes

TWITTER BOTS

Computer generated accounts that are used to increase the visibility of dubious stories on social media

HIGHLY TARGETED ADVERTISING

Ads that are targeted to individuals using personal information harvested from social media sites

A. AN ALLIANCE AGAINST DIGITAL THREATS TO DEMOCRACY AKA A “CYBER NATO”

The low-level cyberwarfare between a handful of states that is perpetually underway turned its attention to political disruption in the past few years.¹⁴ These kinds of attacks are not new. Superpowers have long meddled in foreign elections to secure outcomes that further their objectives. What is new is the level to which information has been weaponized using new digital tools. In addition to being weaponized, those weapons are democratized, so that it is not just superpowers, but also small states and even non-state actors who can deploy them. And these actors can do so under the cover of anonymity, using the West's tradition of respect for privacy as a cover for their activities. Social media and communications technology have overcome geography and distance as impediments to these kinds of attacks and the threat is asymmetric: autocracies are not vulnerable in the same way as democracies are.¹⁵ Therefore, it is in the interest of all nations committed to liberal democratic values to collaborate to protect democracy.

¹⁴ Schmidt, Eric and Jared Cohen. *The New Digital Age: Transforming nations, businesses, and our lives*. Vintage Books, 2014, p.103.

¹⁵ For further description and discussion on Toomas Ilves' Cyber NATO proposal, see Appendix A.

Much as NATO defended citizens and the physical infrastructure of democratic states from an external threat during the Cold War, so we need a “Cyber NATO” to defend the citizens and civic architecture of democracies in all parts of the globe from threats online today. As argued by Ilves, such a commission would best be developed through a new set of institutions no longer bound by geography, as democracies throughout the world, including outside of the North Atlantic region, are similarly threatened.

“Much as NATO defended citizens and the physical infrastructure of democratic states from an external threat during the Cold War, so we need a “Cyber NATO” to defend the citizens and civic architecture of democracies in all parts of the globe from threats online today.”

Effectively counteracting these challenges will require coordination among an alliance of democratic states working together to build cybersecurity defenses, coordinate early warning alert systems and shared intelligence, and potentially coordinate defensive action. The new digital security alliance will require cooperation by technology contractors who develop encryption technology and other systems to be deployed and shared only within the alliance, much like advanced weapons systems developed by Raytheon or Lockheed Martin. Such technology could be used to protect sensitive information,

secure voting systems, and identify and stop hacks, leaks, and the sources of bots and trolls. To improve security and transparency, secure digital identities should be created for all citizens of member countries, such as Estonia has done. To do so will require working with civil society to overcome privacy concerns, particularly in the United States.

Democracies need to work together to create a new form of defense organization, a non-geographical but strict criteria-based organization to defend free and fair elections, preserve the rule of law and guarantee fundamental rights and freedoms.

B. TECHNOLOGY INDUSTRY STANDARDS GROUP

With the weaponization of propaganda and disinformation that the digital communication and information environment has enabled, threatened democracies feel the need to take action.¹⁶ As a result, the technology platform industry faces the prospect of competing and contradictory regulation from various countries that could not only disrupt the digital economy, but also compromise the very democratic values we mean to protect.

As with the maturity of influential industries throughout history, the time has come to establish the rules of the road for the information landscape in order to protect democracy. Just as ICANN was established to oversee the Internet’s growth and development so as to ensure that it remained a network committed to norms of openness and free information sharing, so too should social media and content-sharing platforms participate in multi-

¹⁶ Bentzen, Naja. “‘Fake News’ and the EU’s Response.” *European Parliamentary Research Service Blog*. 2 April 2017, <https://epthinktank.eu/2017/04/02/fake-news-and-the-eus-response/>.

stakeholder consortia to set standards for information quality and promote norms that preserve the public square.¹⁷

Similar to the MPAA for Hollywood or other industry associations, such a group would perform a number of vital functions.^{18,19} As Jerry Kaplan, a Silicon Valley entrepreneur and visiting scholar at Stanford University, argues, such a group could credibly interface with governments to guide and coordinate regulatory responses in a way that no single company could.²⁰ They could also share information to identify sources and tactics of trolls and bots intent on civic vandalism.

“We believe that technology platform companies can mitigate this threat to their core businesses by continuing to increase their responsibility for the social and political consequences of their platforms. A clear signal to do so would be the creation of this industry association.”

The consortium could develop codes of conduct and exert the pressure required for technology platforms to optimize their algorithms to suppress poor quality content. Currently, business models revolve around user engagement (“clicks”) no matter the quality of the content. Fake and misleading news meant to inspire outrage and sow political division is ubiquitous across social media platforms both as a result of human nature and the bots and trolls designed to manipulate them. We need to change this underlying market dynamic to enable real news to compete and win.

From a technical standpoint, it would not be difficult to change the way that social media platforms operate. Algorithms of social media platforms could be adjusted to reduce the virality of fake news or questionable content. The same way Facebook has become incredibly effective at identifying and removing nudity, pedophilic content, and other kinds of offensive material, similar methods could be used for fake news. However, the virality of such content dampens the motivation of technology platforms to take actions that would reduce traffic. The consortium could provide the motivation to make these changes.

¹⁷ The International Corporation for Assigned Names and Numbers (ICANN) is a non-profit public benefit corporation comprised of private, public, civil society, and technical groups dedicated to preserving the operational stability of the Internet, promoting competition, achieving broad representation of global Internet communities, and developing policy. ICANN operates on a “bottom-up, consensus-driven, multi-stakeholder” model, establishing global standards and policies for how the “names and numbers” of the Internet run. ICANN’s international oversight and technical coordination of how these names and numbers are assigned and function is what allows computers to transmit information to one another across the globe and enable the functioning of single, interconnected, global Internet. For more information, see <https://www.icann.org/resources/pages/welcome-2012-02-25-en>.

¹⁸ The Motion Picture Association of America (MPAA) is an American industry consortium representing six major Hollywood studios. Among other lines of work, the MPAA administers the MPAA film rating system, which rates the suitability of a film’s content for certain audiences. According to the MPAA, “Before the rating system was established, filmmakers were encumbered by a bureaucratic system of local, state and federal boards that mandated strict “moral standards” for films in order to be exhibited to the public. These standards often destroyed the artistic integrity of films or, in some cases, kept them from being shown to audiences altogether... When the industry adopted self-regulation, government censorship of films became pointless. The voluntary rating system, which according to former MPAA President Jack Valenti “freed the screen” of regulations and restrictions”. For further description and discussion on the MPAA and the impact of self-regulation, see: <http://www.mpaa.org/the-voluntary-rating-system-promotes-free-speech/#.Wa7SKciGOUk>.

¹⁹ The Extractive Industries Transparency Initiative (EITI) provides global standards on how the extractive industry is governed, promoting open and accountable management of oil, gas, and mineral resources. The EITI is supported by a coalition of governments, companies, and civil society organizations, working together to improve the governance of the extractive sector globally. For more information, see <https://eiti.org/who-we-are>.

²⁰ For further details on Jerry Kaplan’s Industry Standards’ Group, see Appendix B.

In order to identify fake news for the purpose of limiting its virality, third-party fact checking websites, like Snopes, Fact Checker, and PolitiFact could be leveraged to expand how they rate the quality of information online. The consortium could broker collaboration between platforms and fact-checkers to automate scoring content for verifiability and to warn users before sharing questionable content. This must be done in a way that enables the fact checking services to operate independently from the platforms.

In order to cooperate, the culture of competition between technology platform companies must be overcome. This will require courageous leaders in the technology platform industry to step forward to participate and encourage the participation of others. If Mark Zuckerberg of Facebook and Sergey Brin of Google were to stand together to advocate for this, other technology platform company leaders would come on board. Such action is unlikely to occur without significant pressure from both an external public and from the internal employee base of the platform companies.

The greater degree to which technology platform companies can, together, get out in front of these challenges, the greater degree to which they have the ability to shape the regulatory environment that is emerging. Without timely and effective action to preserve the vital role of the public commons in the democratic process, these companies may be facing anti-trust legislation designed to break their monopolies. We believe that technology platform companies can mitigate this threat to their core businesses by continuing to increase their responsibility for the social and political consequences of their platforms. A clear signal to do so would be the creation of a process and institution by which business practices can be balanced with public interests.

2. Rebuilding the Public Square

Social media sites have come to form a part of the public square with a speed that few could have anticipated. Of Americans, 62% now receive news from social media platforms and 18% do so regularly; while in the European Union, 46% of the population gets news from social media.^{21,22} Moreover, Twitter, Reddit, Facebook, and many other similar sites have become platforms for citizens to debate and share information among their networks.

Today, the public square includes a mix of traditional media (some of which is in decline and much of which has lost the trust of the public) and social media, which was not designed to fulfill the functions of the fourth estate. Rebuilding the public square means reforming both of these pillars of our information landscape.

Facebook was designed for social-emotional conveyance, not news or democratic deliberation. Not surprisingly, it performs these roles fairly poorly. Deliberation requires the exchange of different views through civil, rational discussion supported by facts and argument, but that is rarely what happens on social media.²³ Instead, the norms of behavior on major social media platforms encourage polarization and poor quality deliberation, in most cases.

“For our democracies to thrive, citizens must have access to high-quality information and opportunities for deliberative political discourse.”

As outlined above in the introduction—from the questionable quality of information, to the promotion of extreme positions and uncivil discourse, to the narrowing of perspectives and the impact on tolerance and more—the challenges to be managed as political discourse moves to the virtual public commons are ample and varied.²⁴

Meanwhile, print journalism, and the professional journalists they employ, has suffered significant losses during the meteoric rise of digital media. Declining subscriptions for print and the migration of advertisers to Google and Facebook have decimated the revenue models of print media companies resulting in bankruptcies, reorganizations, and the shuttering of local newspapers everywhere.²⁵ Between 2000 and 2015, advertising for print newspapers declined from U.S.\$67 billion to U.S.\$16 billion in the United States.²⁶

²¹ Gottfried, Jeffrey and Elisa Shearer. “News Use Across Social Media Platforms 2016.” *Pew Research Center*. 26 May 2016, <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>.

²² Bentzen, Naja. “‘Fake News’ and the EU’s Response.” *European Parliament Think Tank*. 31 March 2017, http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599384/EPRS_ATAG%282017%29599384_EN.pdf.

²³ Radcliffe, Dana. “Dashed Hopes: Why Aren’t Social Media Delivering Democracy?” *HuffPost*. 21 Oct 2016, http://www.huffingtonpost.com/dana-radcliffe/dashed-hopes-why-arent-so_b_8343082.html. See also, <http://danigayo.info/publications/IEEEMultimedia-DGayo-2015.pdf>.

²⁴ Hampton, Keith, et al. “Social Media and the ‘Spiral of Silence’.” *Pew Research Center*. 26 Aug 2014, <http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/>.

²⁵ Large newspaper chains filing bankruptcy since December 2008 include the Tribune Company, the Journal Register Company, the Minneapolis Star Tribune, Philadelphia Newspapers LLC, Sun-Times Media Group and Freedom Communications. For further description and discussion, see https://en.wikipedia.org/wiki/Decline_of_newspapers#cite_note-24.

²⁶ Thompson, Derek. “The Print Apocalypse and How to Survive it.” *The Atlantic*. 3 Nov 2016, <https://www.theatlantic.com/business/archive/2016/11/the-print-apocalypse-and-how-to-survive-it/506429/>.

For our democracies to thrive, citizens must have access to high-quality information and opportunities for deliberative political discourse. In a diverse society, it is vital that we are exposed to a broad range of perspectives on current issues, not only those that conform to our already held beliefs and prejudices.²⁷ Without sources of information that are broadly trusted, “alternative facts” compete with truth as people choose their sources based on bias.

We need to restore the legitimacy and vitality of professional journalism and educate citizens how to recognize it.²⁸

A. ALIGNING INCENTIVES FOR PRO-DEMOCRATIC SOCIAL MEDIA

As noted above, social media platforms are currently poorly designed to act as sites of civic deliberation and the exchange of reliable information. Instead, they are designed as loud flashing beacons of outrage and entertainment in order to capture clicks in the attention economy.²⁹ Yet, as undesirable as these kinds of behavior are from the point of view of civic deliberation, from the point of view of the social media platforms, they drive traffic.

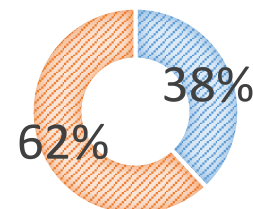
What we face is an incentives problem. The dynamics of the attention economy are disruptive to the public square and potentially destabilizing to democracy. Governments could, of course, legislate to impose restrictions on the information shared over social media platforms, but a more elegant solution would surely be to provide incentives for technology companies to tackle this problem themselves.

One option, suggested by an industry leader during our Washington D.C. meeting, is for advertisers and brands to take an increased interest in the content their products support. Just as advertisers have rightly been reluctant to support pornography or hateful content online, similar concern could be extended to lies, misinformation, and egregious partisanship.³⁰ The technology platforms rely on an advertising model to ensure their growth possibilities and market dominance, thus giving

Where People Get News

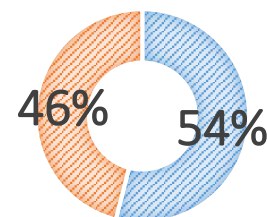
UNITED STATES

■ Traditional ■ Social Media



EUROPEAN UNION

■ Traditional ■ Social Media



²⁷ For further description and discussion, see Sunstein, Cass. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press, 2017.

²⁸ Cohen, Tom and Nathalia Ramos. “Is Old News Fake News.” *The WorldPost*. 18 Jan 2017, http://www.huffingtonpost.com/entry/is-fake-news-old-news_us_587ffcf8e4b0aa1c47ac2817.

²⁹ McDonald, Patricia. “The Attention Economy and the Demise of the Middle Ground.” *The Guardian*. 6 July 2016, <https://www.theguardian.com/media-network/2016/jul/06/attention-economy-demise-middle-ground>.

³⁰ Philp, Bruce. “How Corporate Brands Reluctantly Became our Moral Guides.” *Macleans*. 24 Aug 2017, <http://www.macleans.ca/economy/business/how-corporate-brands-reluctantly-became-our-moral-guides/>.

advertisers a unique lever of influence to affect the incentives underpinning the online information ecosystem.³¹ Mobilized public pressure on companies to take an interest in this problem could help motivate brands to take action on this front.

B. A VIABLE FOURTH ESTATE

We believe that a multifaceted strategy for rebuilding the health of journalism can be developed.

First, we need to find new mechanisms for financially supporting quality journalism. As technology platforms replace news organizations as publishers, their ability to monetize content is reduced. While these platforms afford them larger audiences than they have ever had access to before, this reach does not translate into adequate revenue. There are a number of possible approaches including expanding government support, developing new sources of revenue such as public events and conferences, or transforming media companies into non-profit entities with access to donations from foundations like ProPublica and Kaiser Health News.³² Many such endeavors are underway and media companies and civil society actors are working to find sustainable solutions. Ultimately, the technology platforms will likely need to develop new revenue sharing structures to support content providers as part of the solution set.

“Critical to combatting the threat of disinformation and misinformation is also the vibrancy of a healthy information ecosystem. We must ensure that journalism—on the international, national, and local levels—thrives.”

Second, we must restore public trust in media. As traditional media has struggled to remain relevant and solvent in this exploding digital world, news outlets and broadcast journalists alike have tended increasingly toward promoting sensationalism and partisan bias. Without question, the need to survive in the attention economy has affected content choices and objectivity. And they are paying a price for that. This declining revenue matches a simultaneous decline in trust. According to a recent Gallup poll,

trust in media reached an all-time low of 32% among Americans in 2016.³³ In order to regain the public’s trust, media must strive for objectivity, remain committed to fidelity to the truth, and operate to high standards of quality journalism. Indeed, new revenue models that rely on public funding and private foundations must be tied to such standards of quality.

³¹ For further details on aligning incentives, see Appendix C.

³² ProPublica is an independent, nonprofit newsroom that produces investigative journalism. Unlike most traditional media, it is funded by donors, comprised of individuals, foundations, and funds. For more on how ProPublica is funded, see <https://www.propublica.org/supporters/>. Kaiser Health News is a nonprofit news services focused on in-depth coverage of health policy and politics. It is primarily funded by the Kaiser Family Foundation, a nonprofit private foundation. For more on how Kaiser Health News is funded, see <http://khn.org/fag/>.

³³ According to a Gallup poll conducted in 2016, there has been a collapse in trust in journalism among U.S. Republicans, down to 14% from 32% the previous year. Swift, Art. “Americans’ Trust in Mass Media Sinks to New Low.” *Gallup*. 14 September 2016, <http://www.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx>. Lack of trust in journalism, across the world, however, is a new global phenomenon. For further description and discussion, see Dragomir, Marius. “Trust in Journalists and News Media Sinks to New Lows.” *Media Power Monitor*. 5 June 2016, <http://mediapowermonitor.com/content/trust-journalists-and-news-media-sinks-new-lows>.

Third, we must maintain a pipeline of journalists from all backgrounds that are focused not on providing journalism merely as it was in prior decades, but on journalism that creatively engages the public in the most meaningful manner. Enrollment in journalism schools have been declining for undergraduate and graduate programs alike.³⁴ As media companies shutter their doors, fewer students—or their parents—are electing to invest in an education that is unlikely to lead to employment.

However, there are vast opportunities for young people to become involved in the journalistic enterprise in new media. For example: the rise of social media platforms has allowed for new types of investigative journalism and the development of new forms such as citizen journalism. A prime example in recent times would be with the issue of police violence, which has come to the fore largely because of citizen filming. Such opportunities through formal and informal mechanisms should be developed to enable young people to engage in journalism and expand and enhance these tools.

Critical to combatting the threat of disinformation and misinformation is also the vibrancy of a healthy information ecosystem. We must ensure that journalism—on the international, national, and local levels—thrives.

C. DIGITAL CIVIC LITERACY

In order to arm our democracies against the forces that would seek to disrupt it and help restore faith and appreciation for quality, independent journalism, we must educate citizens. Digital civic literacy remains one of the most important skills in today's economy and in society. Citizens of all ages can fall prey to a number of dangers in this relatively new and ever-evolving digital world.

Digital education has largely focused on giving young people technical skills in computers and programming in order to equip them for jobs in the digital economy.³⁵ More recently digital literacy has expanded to include education in areas of finance, security, sex, bullying, and more. Now it needs to include civics.^{36,37}

³⁴ Lynch, Dianne. "Above and Beyond: looking at the future of journalism education." *The Knight Foundation*. Chapter 2, <https://knightfoundation.org/features/je-the-state-of-american-journalism/>. Accessed on 31 Aug 2017.

³⁵ For further discussion on the current state of digital education, see <http://www.telegraph.co.uk/education/educationopinion/10436444/Digital-literacy-as-important-as-reading-and-writing.html>.

³⁶ For further discussion on enhancing digital education, see <http://mediasmarts.ca/digital-media-literacy-fundamentals/digital-literacy-fundamentals>.

³⁷ Google has developed a digital citizenship program for educators <https://www.google.com/safetycenter/resources/> and the Knight Foundation, together with the Aspen Institute, have made the case for making digital citizenship a part of the core curriculum. See https://assets.aspeninstitute.org/content/uploads/2010/11/Digital_and_Media_Literacy.pdf.

“Governments, educators, and civil society must undertake to educate citizens now in how to recognize questionable content, avoid falling prey to bots and trolls, and establish norms of behavior that sustain democratic deliberation.”

We cannot wait for the next generation to grow up to become responsible digital citizens. Governments, educators, and civil society must undertake to educate citizens now in how to recognize questionable content, avoid falling prey to bots and trolls, and establish norms of behavior that sustain democratic deliberation. A key part of this could be engaging the platforms in playing an educational role on the topic as this would have an immediate impact on large numbers of people.

Digital literacy and civics would include the importance of quality journalism and the role of general interest intermediaries in our democracy, and address the variety of deleterious online activities, such as bullying and hate speech. Wide spread digital civic literacy efforts could establish new cultural norms of behavior in the public space, both on and offline.

3. INNOVATING FOR MORE EFFECTIVE GOVERNANCE

So far our conversation has focused on defending the current system against immediate threats and rebuilding the capacity for quality information and political discourse. Now we turn our attention to adapting our democratic institutions to the digital age.

Exciting initiatives are taking place all over the world to involve citizens more actively in governance, such as Estonia's Rahvakogu, Finland's Open Ministry, or the United States' Peer-to-Patent initiative and the 70-country membership organization Open Government Partnership.^{38,39,40} Many of these initiatives demonstrate that, given carefully designed and facilitated channels, citizens can be an important resource for government, providing their ingenuity, expertise, and resources to support the work of civil servants.

Additionally, online avenues for citizens to petition government are active in the European Union, the United Kingdom, the United States, and beyond. Meanwhile, platforms like Twitter, allow citizens to interact with policymakers and elected officials at the highest level.

The solutions in this section are promising ideas that deserve further exploration. Any solution that involves redesigning our democratic systems is bound to be controversial. Many of these initiatives ask us to rethink the relationship between the governed and those governing. What we advocate is not wholesale redesign of our democracies according to any formula but rather ongoing, brave, and consequential experimentation that aims to improve public trust and participation and enhances capacity for problem-solving.

Innovation should not be seen as optional because the disruption of technology is real and democracy is not immune. We must adapt.

A. REDESIGNING DEMOCRATIC INSTITUTIONS

The design of our democratic institutions—from election processes and procedures to parliamentary norms and policy development mechanisms—can reduce or amplify the polarization, fragmentation, and public distrust that is being augmented by our media and communications environment. Implementation of design that reduces partisanship, enhances collaboration and government effectiveness, and diminishes the potential for mischaracterization should be adopted as adaptations to technological disruption.

While overcoming polarization to make government more effective will likely have the impact of restoring and maintaining trust, there are also design ideas that can overcome distrust by enhancing citizen participation and increasing transparency. The following ideas are not recommendations, rather they are examples of the landscape of possibilities.

³⁸ For further description and discussion on Estonia's public initiatives to engage citizens, see <https://rahvakogu.ee/in-english/>.

³⁹ For further description and discussion on Finland's Open Ministry, see <http://openministry.info/>.

⁴⁰ For further description and discussion on the United States' public initiatives to engage citizens, see <http://www.peertopatent.org/>.

Reducing Polarization and Fragmentation: There are a number of ways to design democratic systems that reduce rather than amplify polarizing forces. Open primaries and ranked-choice voting provide opportunities to appeal to moderates and for more moderate politicians to succeed.⁴¹ In the United States, for example, public financing of elections and equal time provisions for candidates will afford independent and third party candidates an equal footing with candidates from the mainstream duopoly that inevitably become more polarized over time. Elsewhere, requiring politicians to abandon party affiliation once elected and develop procedures that support and emphasize constituent representation over party loyalty once elected could enhance cooperation.⁴² As former U.S. Administrator of the Office of Information and Regulatory Affairs and American legal scholar Cass Sunstein argues in his book *#Republic*, group identity and group membership matter in deliberation.⁴³ When one group is defined in opposition to another, disagreement becomes nearly an automatic reaction to whatever is proposed. By removing party affiliation and redefining participants as representatives and groups as “problem-solvers”, we enhance the possibility of more effective chambers. An extreme version of this is evolving to a post-party democracy which would involve right-sizing districts, stepped voting processes, and a non-partisan council.⁴⁴

Enhancing Citizen Participation: Deliberative polling is one method for involving ordinary citizens in complex and potentially sensitive discussions about governance. Developed by Stanford University’s Director of the Center for Deliberative Democracy James Fishkin, deliberative polling combines the advantages of polling—to quickly gauge the opinions of large numbers of people on a given issues—with the advantages of small group discussions, to allow people to consider facts, evidence, and arguments.⁴⁵ Participants are first asked their opinions on a broad range of topics, then invited to participate in a number of small group discussions before giving their opinions on the same issues a second time. Through social media, this technique could potentially be used at a very large scale to give politicians a more nuanced sense of how citizens see issues.

“While overcoming polarization to make government more effective will likely have the impact of restoring and maintaining trust, there are also design ideas that can overcome distrust by enhancing citizen participation and increasing transparency.”

Another example for how ordinary citizens could play a more active role in deliberating policy comes from the radical fringe. The Pirate Party in Germany uses a form of collective decision-

⁴¹ For further description and discussion on open primaries and ranked-choice voting, see <https://www.forbes.com/sites/realspin/2016/01/14/broken-american-voting-system-ranked-choice-voting/#1d4f1c043b62>. For further analysis on the effectiveness of the aforementioned, see <http://democracyjournal.org/arguments/ranked-choice-voting-is-not-the-solution/>.

⁴² Sunstein, Cass. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press, 2017, p. 73.

⁴³ For further description and discussion on group identity and membership and its effect on deliberation, see Sunstein, Cass. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press, 2017.

⁴⁴ Gardels, Nathan and Nicolas Berggruen. “Post-Party Democracy Can Restore the Rule of the Many over Money.” *HuffPost*. http://www.huffingtonpost.com/nathan-gardels/post-party-democracy_b_5108263.html. Accessed on 1 Aug 2017.

⁴⁵ Fishkin, James S. and Robert C. Luskin. “Experimenting with a Democratic Ideal: Deliberative polling and public opinion.” *Palgrave Journals. Acta Politica* 2005, 40: 284-289. [doi:10.1057/palgrave.ap.5500121](https://doi.org/10.1057/palgrave.ap.5500121).

making dubbed liquid democracy.⁴⁶ Any member of a liquid democracy community can make a proposal relevant to any given issue. Other members of the community may then offer counter proposals or amendments or choose to support the proposal. If the proposal passes a threshold of support, it is put to the whole community for a vote. The second central principle is that individual members of the community, when voting, may choose to cast their own vote or delegate their vote to someone in the community they believe to be better informed than they are. Such a practice gives greater decision-making weight to those who have the greatest expertise on a given issue and allows voters to choose different delegates for different issue areas. Liquid democracy is not a proven design and we are not advocating its use, but, as an experiment in voter participation it may offer lessons for both established parties and new more mainstream movements like *En Marche*.^{47,48}

“Hacking and doxing are the new normal. While the most advanced cybersecurity measures must continue to be rigorously applied, the possibility of a breach must be assumed and considered in all digital communications.”

Digital Norms and Best-Practice Protocols: As pointed out by Tom Pitfield, the President of Canada 2020, during our roundtable discussion in Washington D.C., as communications grow increasingly digital, governments can no longer rely on the complete protection of privacy.⁴⁹ For political leaders and their staffs, hacking and doxing are the new normal. While the most advanced cybersecurity measures must continue to be rigorously applied, the possibility of a breach must be assumed and considered in all

digital communications. In order to protect against the destabilizing impact of these events and the distrust it breeds, very specific protocols around the appropriate mode of communication, given the nature of the content, must be applied with great discipline in all corners of government. Email, texts, phone calls, etc., all have different security exposures and propensity for misunderstanding or vulnerabilities to being taken out of context.

In order to support continued trust in the democratic system, even long-standing democracies, such as Canada, the United States, and France, must consider designing governing institutions to resist the negative forces of a polarized society. Adapting systems to the 21st century can restore faith in the legitimacy of the process and of the politicians that populate it. While we do not advocate any specific step at this juncture, we encourage further research and experimentation to harden democratic systems against the potentially destructive forces in this more vulnerable era.

⁴⁶ The Pirate Party is a German political party established in 2006 that favors the civil right to information privacy and promotes enhanced transparency of government by implementing open source governance and providing for APIs to allow for electronic inspection and monitoring of governments operations by the citizens. For more on the Pirate Party, see <https://wiki.piratenpartei.de/Parteiprogramm>.

⁴⁷ Blum, Christian and Christina Isabel Zuber. “Liquid Democracy: Potentials, Problems and Perspectives.” *Journal of Political Philosophy*. 2005, 24: 162-182, [doi:10.1111/jopp.12065](https://doi.org/10.1111/jopp.12065).

⁴⁸ *En Marche* is a French political party established in 2016 by then Minister of Economy, Industry, and Digital Affairs Emmanuel Macron. Considered a disruptor to French politics, *En Marche* is neither left or right, slated to transform politics and governance as is currently practiced in France. For further description and discussion on *En Marche*, see <http://www.newstatesman.com/culture/2017/06/new-french-revolution-how-en-marche-disrupted-politics>.

⁴⁹ Canada 2020 is Canada’s leading independent, progressive, think-tank. Founded in 2006, Canada produces original research, hosts events, and starts conversations about Canada’s future. For further description on Canada 2020, see <http://canada2020.ca/about/>.

B. CHARISMATIC TRANSPARENCY

One of the drivers for dissatisfaction with government—as well as other institutions—is distrust bred from a sense that elites are self-serving and politicians dishonest. Economic inequality aggravates this and can give rise to populism as political leaders tap into the sense of injustice, making accusations of corruption against political elites. To guard against corruption—and its perception—governments should opt to operate with transparency.

Governments that score well for transparency, such as Denmark, Sweden, Canada, and the United Kingdom, among others, operate according to norms and practices consistent with high standards of openness and oversight.⁵⁰ These might include standards for disclosure, public oversight of budget management, and making publicly available meeting minutes and other procedural records. But these efforts are about complying to legal obligations rather than meeting public needs.⁵¹

ICTs have changed social expectations for communication and interaction between institutions and individuals. The corporate sector has adopted these new tools with vigor, shaping these expectations to some extent. Products, services, information, and feedback are all available with a few clicks and swipes. Moreover, there is a concerted effort to get attention and engage consumers using these tools.

“Charismatic transparency would involve the active implementation of these [ICT] tools to personalize and enhance the experience of government for citizens.”

Charismatic transparency would involve the active implementation of these tools to personalize and enhance the experience of government for citizens. Governments should adopt the tools available to improve interaction, suggest solutions or opportunities for engagement, make citizens aware of public services, and develop user-interfaces that invite

rather than discourage making use of them. Information about how decisions were made could be delivered as explainer videos. Budget allocation could be gamified.⁵² Data visualization could make information more accessible. Legislative hackathons at the local, regional, national, and global level could be employed.

Data transparency presents an opportunity to enhance public trust by engaging citizens solving collective problems. However, it requires more than a data dump. Just publishing reams of undifferentiated data is a start, but is unlikely to speak to citizens or make it easy to generate new breakthroughs. As noted above, we need new types of transparency that actively invites the public to participate in projects, such as Apps4Africa competitions, Global Public Health Intelligence Network, and the Open Data movement have done.⁵³ The

⁵⁰ For further description and discussion on norms and practices of countries with high transparency indexes, see https://www.transparency.org/news/feature/corruption_perceptions_index_2016.

⁵¹ Cucciniello, Maria and Greta Nasi. “Transparency for Trust in Government: How effective is Formal Transparency.” *International Journal of Public Administration*. 2014. 37: 911-921. doi: 10.1080/01900692.2014.949754.

⁵² The State of California gamified its 2012 state budget to assess how constituents would allocate financial resources.

⁵³ Apps4Africa is an African innovation accelerator that funds projects that use technology to solve local or global problems. For more on Apps4Africa, see <https://en.wikipedia.org/wiki/Apps4Africa>. Global Public Health Intelligence Network (GPHIN) is an early warning system for potential public health threats worldwide. Operating 24 hours a day, seven

opportunity and challenge of information superabundance we face, requires resources and human ingenuity. Government alone cannot tackle it, but they play a vital role in making the data itself accessible.

In practice this is difficult to achieve. Making sense of information superabundance is not easy and requires technical expertise. New centers for civic analytics would harness Big Data for the public good, providing policymakers with the tools to better understand the challenges they face and the impact of the interventions they make.

Most of the ideas listed here are not brand new. Indeed, there is a great deal of innovation going on in different countries and regions to adopt technology and connect with constituents and citizens. But few governments have adopted an entirely new conception of its obligation for transparency or how to accomplish it. Adapting to the expectations and limitations of an overwhelmed public immersed in the cacophony of the digital world will require charismatic and proactive transparency on the part of democratic governments. Political stability and public trust demand it.

days a week, GPHIN is curated by human analysts who monitor media sources across the globe to provide organized and relevant information to users. For more on GPHIN, see https://gphin.canada.ca/cepr/listarticles.jsp?language=en_CA. The Open Data movement promotes citizen's rights to access and reuse government information. The movement rests on the idea that data is as much a public asset as a highway, bridge, or park and so should be made available to those who paid for its creation and curation: taxpayers. For more on the Open Data movement, see http://www.slate.com/articles/technology/future_tense/2012/09/open_data_movement_how_to_keep_information_from_being_politicized_.html.

CONCLUSION: RENOVATING DEMOCRACY FOR THE DIGITAL AGE

Just as leaders and citizens responded to the challenges of the Industrial Era with a new conception of democracy and a broader social contract, so too must leaders and citizens respond to the Digital Era with a new “solution set” for democracy today. The Berggruen Institute’s project team on Renovating Democracy for the Digital Age has undertaken over the past year an initial attempt to identify some of the possible solutions to the challenges we face.

These ideas need further development and testing with a broad array of stakeholders. In addition to expanding the conversations in Canada, Europe and beyond, the project team also hopes to engage the broader public potentially through an online platform.

Specifically, we will be investing in further exploration of:

1. A “Cyber NATO”;
2. A technology industry standards consortium; and
3. Digital Civic Literacy programs focused on developing an approach to digital literacy that includes a focus on civics.

A first step in moving this agenda forward could be the development of a multi-stakeholder process involving governments, firms, and civil society representatives which seeks to provide a location where urgently needed voluntary steps can be taken by all parties on all of the above ideas. This multi-stakeholder process could bring together both the ‘cyber-NATO’ and the technology standards consortium.

While we believe that all of the ideas contained within this preliminary solution set merit further exploration, we believe that these proposals have potential to gain traction among concerned stakeholders. The Berggruen Institute, in concert with our partners, is eager to use our convening power to facilitate progress in these areas immediately, even as work on additional solutions proceeds apace.

GLOSSARY

Attention Economy: A new marketplace that treats human attention as a scarce commodity and resource. With the advent of social media and online news, eyeballs, or page-views and clicks, are the new currency.⁵⁴

Disinformation: False information deliberately and often covertly spread in order to influence public opinion or obscure the truth

Fake News: False, often sensational, information disseminated under the guise of news reporting

Fourth Estate: Journalist profession and its members; the press and media

Misinformation: False or incorrect information that is spread intentionally or unintentionally, without realizing it is untrue

Technology Platform: A digital platform business that creates value by facilitating exchanges between two or more interdependent groups, usually consumers and producers. Platforms don't usually own the means of production—instead, they create the means of connection.⁵⁵

⁵⁴ For more on the attention economy, see <https://www.theguardian.com/media-network/2016/jul/06/attention-economy-demise-middle-ground>.

⁵⁵ For more on technology platforms, see <https://www.applicoinc.com/blog/what-is-a-platform-business-model/> and <https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html>.

NOTES

Bell, Emily and Taylor Owen. "The Platform Press: How Silicon Valley Re-engineered Journalism" *Tow Center for Digital Journalism*. 29 March 2016, www.cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php. Accessed on 26 April 2017.

Bentzen, Naja. "'Fake News' and the EU's Response." *European Parliamentary Research Service Blog*. 2 April 2017, <https://epthinktank.eu/2017/04/02/fake-news-and-the-eus-response/>.

Blum, Christian and Christina Isabel Zuber. "Liquid Democracy: Potentials, Problems and Perspectives." *Journal of Political Philosophy*. 2005, 24: 162-182, [doi:10.1111/jopp.12065](https://doi.org/10.1111/jopp.12065).

Castells, Manuel. *The Rise of the Networked Society*. Wiley-Blackwell. 2010, p. 97.

Cohen, Tom and Nathalia Ramos. "Is Old News Fake News." *The World Post*. 18 Jan 2017, http://www.huffingtonpost.com/entry/is-fake-news-old-news_us_587ffcf8e4b0aa1c47ac2817.

Cucciniello, Maria and Greta Nasi. "Transparency for Trust in Government: How effective is Formal Transparency." *International Journal of Public Administration*. 2014. 37: 911-921. doi: 10.1080/01900692.2014.949754.

Dragomir, Marius. "Trust in Journalists and News Media Sinks to New Lows." *Media Power Monitor*. 5 June 2016, <http://mediapowermonitor.com/content/trust-journalists-and-news-media-sinks-new-lows>.

Fish, Stanley. "Anonymity and the Dark Side of the Internet." *New York Times*. 3 Jan 2011, <https://opinionator.blogs.nytimes.com/2011/01/03/anonymity-and-the-dark-side-of-the-internet/>. Accessed on 11 May 2017.

Fishkin, James S. and Robert C. Luskin. "Experimenting with a Democratic Ideal: Deliberative polling and public opinion." *Palgrave Journals*. *Acta Politica* 2005, 40: 284-289. [doi:10.1057/palgrave.ap.5500121](https://doi.org/10.1057/palgrave.ap.5500121).

Gandour, Ricardo. "Study: Decline of traditional media feeds polarization." *Columbia Journal Review*. 19 Sep 2016, https://www.cjr.org/analysis/media_polarization_journalism.php. Accessed on 26 April 2017.

Gardels, Nathan and Nicolas Berggruen. "Post-Party Democracy Can Restore the Rule of the Many over Money." *HuffPost*. http://www.huffingtonpost.com/nathan-gardels/post-party-democracy_b_5108263.html. Accessed on 1 Aug 2017.

Gottfried, Jeffrey and Elisa Shearer. "News use Across Social Media Platforms 2016." *Pew Research Center*. 26 May 2016, <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>. Accessed on 26 April 2017.

Hampton, Keith, et al. "Social Media and the 'Spiral of Silence'." *Pew Research Center*. 26 Aug 2014, <http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/>.

Lenarz, Julie. "Russia Has Made Fake News into a Weapon That Threatens Democracy in Europe." *The Telegraph*. 26 Jan 2017, <http://www.telegraph.co.uk/news/2017/01/26/russia-has-made-fake-news-weapon-threatens-democracy-europe/>.

Lynch, Dianne. "Above and Beyond: looking at the future of journalism education." *The Knight Foundation*. Chapter 2, <https://knightfoundation.org/features/je-the-state-of-american-journalism/>. Accessed on 31 Aug 2017.

Madoff, L. C., and Woodall, J. P. (2005). "The Internet and the Global Monitoring of Emerging Diseases: Lessons from the first 10 years of ProMED-mail". *Archives of Medical Research*. 36(6), p. 724–30.

McDonald, Patricia. "The Attention Economy and the Demise of the Middle Ground." *The Guardian*. 6 July 2016, <https://www.theguardian.com/media-network/2016/jul/06/attention-economy-demise-middle-ground>.

Mcluhan, Marshall. *Understanding Media: The extensions of man*. MIT Press, 1994. Chapter 1, <http://web.mit.edu/allanmc/www/mcluhan.mediummessage.pdf>.

Philp, Bruce. "How Corporate Brands Reluctantly Became our Moral Guides." *Macleans*. 24 Aug 2017, <http://www.macleans.ca/economy/business/how-corporate-brands-reluctantly-became-our-moral-guides/>.

Radcliffe, Dana. "Dashed Hopes: Why Aren't Social Media Delivering Democracy?" *HuffPost*. 21 Oct 2016, http://www.huffingtonpost.com/dana-radcliffe/dashed-hopes-why-arent-so_b_8343082.html. See also, <http://danigayo.info/publications/IEEEMultimedia-DGayo-2015.pdf>.

Schmidt, Eric and Jared Cohen. *The New Digital Age: Transforming nations, businesses, and our lives*. Vintage Books, 2014, p.103.

Silverman, Craig. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook." *Buzzfeed*. 16 Nov. 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.khXXlenYO#.abvLE29j8. Accessed 28 Aug 2017.

Sunstein, Cass. *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press, 2017, p. 73.

Swift, Art. "Americans' Trust in Mass Media Sinks to New Low." *Gallup*. 14 September 2016, <http://www.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx>.

Thompson, Derek. "The Print Apocalypse and How to Survive it." *The Atlantic*. 3 Nov 2016, <https://www.theatlantic.com/business/archive/2016/11/the-print-apocalypse-and-how-to-survive-it/506429/>.

"Estonia Takes the Plunge: A national identity scheme goes global." *The Economist*. 28 June 2014, <https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge>. Accessed on 11 May 2017.

"Government at a Glance 2017." *OECD Publishing*. 2017, http://dx.doi.org/10.1787/gov_glance-2017-en.

"Today's Washington Press Corps More Digital, Specialized." Pew Research Center. 3 Dec 2015, <http://www.journalism.org/2015/12/03/todays-washington-press-corps-more-digital-specialized/>. Accessed on 26 April 2017.

Appendix A

Towards a Cyber “NATO”: Securing liberal democracies in the Digital Age

Toomas Hendrik Ilves
Distinguished Visiting Fellow, the Hoover Institution
President of Estonia 2006-2016

The digital era, with all of its benefits, has profoundly changed the security environment of liberal democracies. We face potential destruction of national infrastructures and militaries in ways unimaginable a quarter century ago. Even the electoral process in a number of democracies has come under severe threat, with attempts to alter outcomes in a number of elections in the past two years.

The threats are asymmetric: liberal democracies with free and fair elections are vulnerable to attack; autocratic societies, where all that matters is who counts the votes are not. Liberal democracies thus cannot respond in kind to attacks on their way of governance.

Moreover, in the digital era, physical distance and national boundaries have lost their relevance. NATO is the North Atlantic Treaty Organization for a reason: it is a defense organization of liberal democracies in a geographical space, constrained *inter alia* by tank logistics, bomber ranges, the placement of troops. Liberal democracies with free and fair elections such as Japan, Australia or Uruguay cannot belong to NATO simply because of their location. Yet these countries’ critical infrastructure today is as vulnerable as any in Eastern Europe. Their democracies and elections are under no less threat than the U.S. or Germany.

Threats, however, can affect anyone. Only one Russian cyber operation, APT 28 or “Fancy Bear”, has attacked servers of ministries, political parties and candidates in the U.S., Germany, the Netherlands, Sweden, Ukraine, Italy and France and indeed even the servers of the International Association of Athletics Federations responsible for anti-doping monitoring. Military communications have also been targeted by APT 28. Yet APT 28 is but one of numerous such groups from Russia alone. Nor is Russia the only authoritarian government seeking to increase its advantage through cyber operations. It is also clear that Iran has carried out its own offensive cyber operations. Chinese, primarily PLA-affiliated groups have targeted militaries as well as intellectual property in companies the world over.

In other words, the digital age also has ushered in an era of new security threats, perhaps imaginable but not seen until the past decade. Governments, meanwhile, have been slow to respond; multilateral organizations such as NATO and the EU have been slower. Meanwhile international organizations such as the UN, either through the ITU or the UNGGE, simply have failed even to broker a treaty arrangement to prevent the use of digital weapons.

The response, this paper argues, is for a new “Cyber NATO”, a coalition of liberal democracies that better meets the ubiquity of threats. This will be difficult to achieve, yet the alternatives are worse.

1. “Cyber” as a New Threat to Security

The past decade has upended our understanding of traditional security as well as the security of electoral democracy. Our institutions responsible for these have not been up to the task, indeed they have failed to understand the gravity of the changes.

While cyber attacks have taken place for nearly forty years, they were generally carried out for espionage, not to create damage to adversaries or make a political point. It has been just 10 years since the first cyber attack affecting the security of a country and its citizens. Virtually every history of what is now known as “Cyber war” or “Cyber warfare” begins with an account of an attack on Estonia in 2007, when the country’s governmental, banking and news media servers were paralyzed with “distributed denial-of-service” or “DDOS attacks,” blocking citizens access to virtually all major online and digitally based services. Cyberattacks have a far longer history of course, but this case was different: it was overt and public. It was digital warfare, in the well-known definition of the theoretician of war, Carl von Clausewitz as “the continuation of policy by other means,” meant as punishment for the Estonian government’s decision to move a Soviet-era statue from the center of the capital.

Since 2007 overt cyberwarfare and the continuation of policy by other means has proliferated and in ever more virulent form: attacks blanking out regions preceding bombing in conflict zones with DDOS attacks (Georgia 2008); crashing electrical grids (Ukraine 2016, 2017); private companies (Sony 2015), hacking into parliaments (the *Bundestag* 2015 and 2016); political think tanks and parties before major elections (the Democratic and Republican National Committees 2015-2016), presidential candidates (Hillary Clinton 2016, Emmanuel Macron 2017), government ministries (Dutch ministries, Italy’s Foreign office 2016-2017, the U.S. Departments of State and Defense). In one especially egregious case, the records of 23 million employees of the U.S. Federal government were stolen in what is known as the “Office of Personnel Management hack”. Recent testimony and leaks in the U.S. report attempts by a foreign power to delete or alter voter data in 21 (or possibly 39) states before the U.S. presidential elections. These represent merely the attacks admitted to by the victims, not those unreported.

A decade ago, the idea of a major cyberattack was strictly hypothetical. In fact, NATO was originally skeptical about the attack on Estonia in 2007. Since the recognition of politically motivated DDOS attacks and their paralyzing impact, the focus of cybersecurity has shifted to more elaborate possibilities such as the use of malware to shut-down or blow-up critical infrastructure: electricity and communication networks, water supplies, even disrupting traffic light systems in major cities. This goes beyond DDOS and requires “hacking”, as we know the term—breaking into servers or a computer system, not merely blocking access as in DDOS. Indeed, the vulnerability of critical infrastructure became the primary focus of government and private sector concern.

These kinds of cyber attacks could mean shutting down a country, or its military, rendering it then open to unopposed conventional attack. In 2010 the Stuxnet worm, which spun Iranian plutonium enriching centrifuges out of control warned us of the power of cyber to do serious damage to physical systems. Leon Panetta, U.S. Secretary of Defense from 2011 to 2013, warned in 2012 of the potential of a “Cyber-Pearl Harbor”. Subsequent events such as the

shutting down of a Ukrainian power plant in 2016 and again this year through cyber operations showed that such concerns were hardly unwarranted.

At the same time, it's worth noting that one could already do considerable damage to national security and the private sector without disabling infrastructure; the hack of Sony Pictures and of the Office of Personnel Management hack are good examples of an extremely dangerous breach that endangers a country's national security or its commerce.

From these examples, we can see that "cyber attacks" as a term is a catch-all, spanning a range of severity, from attacks that could destroy a nation's critical infrastructure on the extreme side to subtler attacks: hacking politicians, leaking compromising information and jeopardizing election integrity.

2. Responses, National, and Multilateral

Recognition of threats in the digital world has been slow in coming. Although the U.S. and others foresaw potential threats in the early 1990s, and hostile hacking had already been detected by then, they remained in the background. As mentioned, NATO was initially reluctant to address, much less admit, the existence of the country-wide attack on Estonia in 2007. In security policy circles it was only as late as 2011, that Munich Security Conference, the West's premier forum of security policy-makers, held its first panel on cybersecurity.

All of these concerns have fallen under the broad rubric of symmetrical warfare. Whatever they did to you, once you figured out who "they" were, you could do back to them. Cyberattacks were all in the realm of traditional warfare but in a new "domain". The U.S. in 2010 declared "Cyber" the Fifth Domain of Warfare (after land, sea, air and space). NATO at its summit in Warsaw in 2016 declared "Cyber" as its Fourth Domain. Moreover, the U.S. Department of Defense has explicitly said in its cyber strategy that a cyberattack described here need not be met in the cyber domain; thereby sanctioning a kinetic response to a digital threat.

While NATO has acknowledged the potential threats of cyber and propaganda, it has done little operationally. NATO did set up a Center of Excellence in Cyber Security in Tallinn, Estonia and later a similar Center for Strategic Communication in Riga, Latvia. Yet even within NATO, there has been limited co-operation in practices in traditional military operations.

3. Democratic Processes under Attack

It has been only a year since a broader consensus has emerged - at least among intelligence agencies and security policy experts - that electoral processes themselves have come under attack. Manipulations have included "doxing" or publishing materials obtained through hacking as seen in the case of Hillary Clinton and Emmanuel Macron. Such tactics have been bolstered by manufacturing "fake news" on an industrial scale and propagating these through "bots" or robot accounts in social media. Gaining currency, these can be further propagated by real users. One study showed that in the three months leading up to the U.S. election, some 8.7 million fake news stories were shared by users on Facebook while 7.3 million genuine stories were shared. More worrisome is the prospect of voting manipulations

through hacking of unsecured voting machines and by altering or deleting voter data, as both the Department of Homeland Defense and a leaked NSA memo have averred.

In truth, propagation of fake news stories need not be tied to elections and no longer are. Instead they can simply be used in an attempt to sway public opinion. The #SyriaHoax hashtag, alleging Syria's use of chemical weapons in Spring 2017 was a Western hoax, spread virally on Twitter via Twitter-bots. Fake news regarding NATO troop assignments in Eastern Europe today are everyday occurrences. In the French election campaign in Spring 2017, bots and fake news accounts spread scurrilous lies about one candidate, Emmanuel Macron, while leaving his primary opponent, Marine Le Pen, untouched.

How to Respond?

As the past several years in this new digital age have shown, the threat landscape facing democracies has dramatically changed, ranging from traditional threats such as destruction or incapacitation of critical infrastructure to what may be termed soft threats, the manipulation of electoral democracy and public opinion.

Two fundamental differences with pre-digital threats emerge:

First, geography or physical distance, a key determinant of security since the beginning of conflict, has become irrelevant. Proximity to threats or hostile actors has been a primary motivator in security policy for as long as people have been thinking about these issues. Countries traditionally have invaded or been attacked by neighbors, not by adversaries from far away. Indeed, until the age of ICBMs, distance from threats was the greatest source of security, proximity the greatest vulnerability.

This is no longer true. Digital threats do not recognize distance. One is just as vulnerable half the globe away as next door to an adversary. One implication of this is that the earlier basis of alliances, be they NATO or Sparta's Peloponnesian League, weaken or even disappear in the digital age. Everyone is equally vulnerable to attack, regardless of physical distance.

Nor are digital attackers constrained by borders. If the same group of digital attackers can target countries in Europe and the U.S. as well as an international organization dealing with doping in sports, it is clear that "cyber" is a tool that can be used anywhere. After all, if the vulnerabilities are the same, why be constrained by distance?

Secondly, in the digital era liberal democracies are far more vulnerable to asymmetric attacks from autocratic states than before. Propaganda, fake news, disinformation are all as old as the Trojan Horse, yet most of what was considered disinformation as late as the 20th Century, had little effect. In the pre-digital age, disinformation could not easily be propagated. Fake news could not swamp and overwhelm the news media. Election rolls could not be manipulated on a massive scale and across many election districts.

Moreover, only liberal democracies are fundamentally vulnerable to attacks and manipulations of the electoral process. Authoritarian governments need not fear external manipulations of electoral processes as these are anyway manipulated by those in power. While it would be difficult to imagine a liberal democracy employing the same methods

against Russia as it used in the U.S. and French presidential elections, attempting to do so simply would have no effect. To have an effect, one needs free and fair elections to affect.

From a security policy perspective, however, the possibilities of using digital manipulations can be quite attractive to an adversary. Why bother with military interventions or attacks (even digital attacks for that matter), if it suffices to use digital means to get a candidate or even a political party in office that does your bidding or at least will follow a policy line favorable to you? Certainly a Le Pen in France or the defeat of Angela Merkel in the upcoming German elections would do more to disrupt European policy toward Russia than any kind of military action.

An Alliance of Democracies in the Digital Age

It is in light of these developments in this age of “cyber” that democracies need to think beyond the hitherto geographical bounds of security. Until now, security was constrained by geography: NATO is the North Atlantic Treaty Organization because that’s where the threats were; these threats were kinetic and by definition constrained by physical distance.

Today, unconstrained by the limits of kinetic war, by the range of missiles and bombers, by the logistics needed to support an armored division, we can succumb instead to digital aggression where physical distance no longer has any meaning. The range of threats we have seen in the past decade since Estonia was attacked digitally—from DDOS attacks to wiping out communications or power grid infrastructure to disrupting elections—are all independent of distance from the adversary.

Disruptions of electoral processes differ, however, because of the asymmetrical vulnerabilities of democracies to the kind of behavior we have witnessed in the past year, behaviors we now see rolled out against European democracies as well.

Thus, we need to rethink our security to take into account these new threats. In addition to those already in existence, we need a new form of defense organization, a non-geographical but a strict criteria-based organization to defend democracies, countries that genuinely are democracies as defined by free and fair elections, rule of law and the guarantee of fundamental rights and freedoms.

This idea is not new, yet earlier proposals predate the digital era, guided more by a philosophical approach than hard security concerns. In different contexts, both Madeleine Albright and John McCain at the turn of the century proposed the creation of a community or league of democracies. Neither proposal went far at the time. The threats to democracies were not of the type described here; neither proposal was based on security concerns. Today, every liberal democracy is potentially vulnerable, none is more secure because of physical distance.

Could such an organization do the job of tackling this new threat? I proposed five years ago at an Atlantic Council seminar at the Munich Security Conference that we consider a cyber defense and security pact for the genuine democracies of the world. After all, Australia, Japan,

Uruguay and Chile, all rated as free democracies by Freedom House, are just as vulnerable as NATO allies such as the United States, Germany or my own country.

The prospects more moving in the direction of safeguarding democracies in the digital era are probably better now than even a year ago. Nonetheless, until this is taken up by the governments of major countries, both in NATO and outside the Alliance, liberal democracies will remain vulnerable to the new threats of the 21st century.

Appendix B

Social Media Industry Consortium Proposal

Jerry Kaplan

Center for Democracy, Development, and the Rule of Law

Freeman Spogli Institute

Stanford University

Advances in technology and the rise of the Internet pose new challenges for civil society. The effective exercise of democracy requires an informed electorate that seeks consensus through open dialog, free of interference and intimidation. While social media has enabled broader participation in public discussion, it has also empowered extremists and demagogues, undermined confidence in sources of news, and given foreign actors new tools for undermining and disrupting democratic institutions. As the “public commons” migrates online, its historic role in the democratic process must be preserved. Social media companies should collectively embrace this civic responsibility.

Today, the industry faces the prospect of ill-conceived and inconsistent regulation in diverse jurisdictions; public criticism for failing to act; hostility to its Silicon Valley roots; and a lack of consensus on how to address these challenges. Existing laws designed to protect social media companies and facilitate their growth now hamper their ability to act. Incubated in an ethos of open competition and free markets, the dominant companies are culturally averse to collaboration and coordinated action. Yet, current trends demand precisely such a response.

Because the industry lacks a single voice or a joint plan to address these issues, numerous governmental agencies and civil groups are stepping in to fill this void with meetings, studies, proposals, and legislation. But they are not the ones best suited to address the problems. Only the industry itself has the data, resources, and ability to take effective action.

A possible path forward is for social media companies to fashion an industry consortium to tackle these issues. Such a consortium can provide the breathing room companies need to implement practical solutions appropriate to their respective communities, share information and best practices that strengthen their individual efforts, and communicate credibly with government agencies as well as the general public.

An industry consortium could:

- *Articulate shared principles and goals.* This serves both as a public relations statement and as conceptual guidance for internal operating groups to align their efforts around common objectives.
- *Provide proactive guidance to regulators.* Government officials around the world are under public pressure to “do something”, though they often lack the knowledge, experience, and ideas required to craft effective solutions. A consortium can speak with greater authority than any individual company, avoid duplication of efforts or working at cross purposes, educate regulators about challenges and approaches, communicate progress on active initiatives, and

advocate for the interests of the industry in the context of serving the public. Today's approach of reacting to regulatory threats as they emerge is unlikely to yield a positive outcome.

· *Increase the effectiveness of company efforts by sharing information and best practices.* Today, armies of paid commenters use fake identities to inject partisan, polarizing or destabilizing content into social media forums for political or financial gain, often using automated techniques for generating accounts and content. While each platform has its own techniques for countering these efforts, their adversaries have the advantage of repurposing their investment across multiple venues, locales, and languages. An industry consortium can help fight fire with fire, by permitting platforms to share relevant threat information legally and confidentially. Pooling information allows the work of each to benefit all, while raising the costs of such attacks for perpetrators. Each company need not independently bear the full cost of countermeasures, and their efforts can be far more effective if relevant information is shared, as it is today in response to cybersecurity threats and email spam.

· *Identify, evaluate, and encourage third-party sources of "signals intelligence".* There are a growing number of independent organizations developing tools to combat disinformation. These include efforts to identify trustworthy sources of news, detect suspicious cross-platform spikes in political activity, and objectively measure inflammatory or harassing user-generated content. Most are working with dribs and drabs of data made publicly available by the platforms. An industry consortium can coordinate, monitor and assist these efforts, as well as help member companies select and apply appropriate tools within their products.

· *Promote safe-harbor website policies and consistent user-interface practices.* As was done for privacy policies and child protection, a consortium can propose standard language for services' Terms and Conditions of Use, and seek applicable legal endorsements. It can also offer common user interface widget and icon designs for useful functions such as indicating that a user's identity has been verified, linking to third-party news source and fact-check ratings, or flagging potentially deceptive content. This promotes consistent, cross-platform user experiences as do shopping carts, thumb-ups and downs, and locks to indicate that secure communication protocols are in effect.

Next Steps

- Secure senior executive buy-in at major social media companies for exploring the formation of an industry consortium.
- Convene a closed-door meeting of responsible representative from as many such companies as practical. CDDRL would be happy to host or facilitate such a meeting.
- Companies could send a representative from public policy or legal departments, and a line executive from each relevant operating division.
- Establish a means for participants to exchange ideas freely and confidentially to assess whether further action is desirable and warranted.

Appendix C

Disrupting the Economics of Misinformation

Vinny Green
Vice President, Snopes.com

In the digital age, misinformation is both a product and a weapon. As publishers of news and fact checks, we naturally oppose *productized* misinformation, which deprives legitimate news organizations of available advertising revenues and exposure and instead funnels it to those who cynically spread lies for self-enrichment. As citizens of the world, however, we are more concerned with countering *weaponized* misinformation, whose purveyors are undermining our collective ability to confront critical challenges and formulate solutions to them. Although the latter may be the more important effort, the former is a necessary—and extremely strategic—step in eliminating the noise of monetized misinformation that drains considerable resources and detracts from our collective ability to target weaponized misinformation.

The “attention economy” and programmatic advertising have ushered in the opportunity for anyone to generate income from digital content by selling advertising space and audience data. Unfortunately, those who peddle misinformation can currently generate revenue from the consumers they reach almost as much as the producers of legitimate news can — with considerably less overhead.

When misinformation is a product offered and bought in the marketplace, the responsibility for its effects stretches far beyond its producers: everyone involved in the transaction (even if unwittingly) is complicit in some way, including the brands that purchase advertising space on the sites that disseminate it, the discovery platforms that provided the exposure to this content, and the service providers who facilitate the transactions. The consumer of misinformation is a victim of the unabated efforts of cynics who spy fruitful opportunities. Removing the financial incentive from the misinformation equation will allow us to more effectively address the more troubling issue of state-sponsored misinformation by sidelining its mercenary peddlers.

One commonly offered viewpoint is that to combat the scourge of misinformation, we simply need “more”: more journalists, more editors, more newsrooms, more accurate reporting, and more compelling storytelling will stifle the spread of misinformation and force it to languish in obscurity amidst a flood of credible content. But that approach cannot work when credible content is not rewarded and respected in the digital ecosystem and thus cannot outperform misinformation in all the metrics that matter to web publishers.

Targeting productized misinformation is an achievable free-market solution that only requires the collective efforts of businesses who control the distribution and monetization of content, and people who consume it. The foolhardy approach would be to attempt to legislatively or

legally bludgeon businesses believed to be complicit in the proliferation of misinformation; they vigorously defend themselves before they admit wrongdoing, and do so with the full weight of their influence and wallet. Instead, we should leverage consumer pressure by publicly exposing the complicit players while simultaneously educating advertisers on the perils of associating with misinformation.

The advent of programmatic advertising (i.e., the automated selling and buying of ad inventory) has created a situation where any reasonable brand safety and credibility standards are either unenforceable or ignored in the digital marketplace. Directing our efforts to programmatic advertising and pressuring advertisers and service providers into divesting themselves from the misinformation ecosystem — thereby denying those who traffic in misinformation from access to scalable revenue and exposure — would be our most effective approach to reducing the volume of online misinformation.

Our efforts should concentrate on those who hold the most influence in the programmatic marketplace. It should not be a surprise that select few advertisers have incredible influence over the entire ecosystem. The focus should be on powerful brands like Kimberly-Clark, Conagra, Procter & Gamble, American Express, Unilever, and L’Oreal, and agencies like WPP, Publicis Groupe, and Interpublic. Any substantive actions from them would be enough to compel even the seemingly untouchable—like Facebook and Alphabet—to act quickly, and would sway service and technology providers like AppNexus, MediaMath, Rubicon, or The Trade Desk, and content discovery engines like Taboola and Outbrain. Even companies that provide hosting solutions like GoDaddy and Hostgator will act before they are subject to intense consumer scrutiny.

We should begin with the following lines of approach:

- Devising campaigns to help educate consumers and advertisers understand the severity of the misinformation problem, the costs (both financial and societal) of associating with it, and the effects it is having on our political discourse and democratic institutions.
- Designing and promoting the adoption of brand safety/credibility standards that enlist digital publishers, advertisers, service providers, and discovery platforms into pledging a commitment to stop the distribution of misinformation for monetary gain.
- Developing technology, resources, and datasets that can be wielded by advertisers, watchdogs, journalists, and everyday citizens to hold those complicit in the proliferation of misinformation accountable.

The cumulative results will fundamentally disrupt the economics of the misinformation, dramatically reduce its volume, and allow us to dedicate a greater portion of our collective effort to investigating state-sponsored disinformation. Furthermore, it will encourage redistribution of revenue and reach to producers of legitimate news and reliable content.

Appendix D

The Social Infrastructure

Eric Klinenberg

Professor of Sociology and Director of the Institute for Public Knowledge
New York University

Social infrastructure is the set of physical places and material systems that shape our face-to-face interactions. Infrastructure is not conventionally used to identify the underpinnings of social life. This is a consequential oversight, because the built environment—not just cultural preferences or voluntary organizations—influences the quality, quantity, and temporality of our associations. The problem isn't only a lack of understanding: If states and societies do not recognize the social infrastructure, they will fail to see a powerful way to promote civic life, within communities and across groups.

The classics of social theory, as well as reams of scholarly research, show that social cohesion develops through repeated interaction and joint participation in shared projects, not merely from a principled commitment to abstract values and beliefs. For decades, concerns about atomization have sparked exhortations for greater community participation from prominent voices in all parts of the modern world. Yet moral suasion has failed to change the way we engage in the neighborhoods and local institutions where we spend our days, the places where democracy begins. Why? In part because cultural values, and exhortations to change them, are by no means the only influences on our everyday social routines and practices. People with the same interest in social connection, community-building, and civic participation have varying opportunities to achieve it, depending on conditions in the places where they live. People form solidarity in places that have healthy social infrastructure—not because they set out to build community, but because when people engage in recurrent interaction, particularly while doing things they enjoy, relationships inevitably grow.

What counts as a social infrastructure? Public institutions, such as libraries, schools, playgrounds, parks, athletic fields, and swimming pools, are vital parts of the social infrastructure. So, too, are sidewalks, courtyards, community gardens, and other spaces that invite people into the public realm. Community organizations, including churches and civic associations, act as social infrastructures when they have an established physical space where people can assemble. Commercial establishments can also be important parts of the social infrastructure, particularly when they operate as “third spaces” (like cafes, diners, barber shops, and bookstores) where people are welcome to congregate and linger regardless of what they've purchased.

Physical infrastructure can be part of the social infrastructure, depending on how it's designed and used. Take the case of levees. A simple levee is an artificial embankment made of less permeable material that prevents water from going where it isn't wanted. This kind of levee is a physical infrastructure that protects social life on the dry side, not a robust social infrastructure. But a levee can be designed differently, and often is. In the late 1930s, for instance, engineers needed to protect Washington D.C. during a spell of heavy rains that led

to massive urban flooding. They could have put up a narrow mound of soil, but instead they built the Potomac Park Levee, a sloped walking path capped by a curved stone wall. In subsequent years it became one of the most popular public spaces in the city, a place where thousands of people go daily without even knowing that they're on top of a critical infrastructure. Today, a growing number of architects and engineers are designing plans for hard infrastructure, such as seawalls and bridges, that incorporate innovative social infrastructure programs, like parks, walking trails, and community centers. These projects, which already exist around the world, provide multiple benefits, from protecting against inundation to promoting public life.

Consider, for instance, the plan for safeguarding and revitalizing Lower Manhattan that came out of the U.S. Rebuild By Design competition, for which I was research director. The Big U, designed by the Danish architect Bjarke Ingles, relies on a series of protective walls that double as sloped parklands, recreational facilities, and aesthetic amenities. It's divided into three sections, each called a compartment, and the design ideas for each site grew out of extensive consultations with local residents, businesses, and community organizations. The compartment on the Lower East Side, which is, for now, the only funded part of the project, features lushly planted berms that protect neighborhoods, infrastructure, and institutions near the river, while also bridging them over a highway to new amenities on the water's edge. The berms would block and absorb storm surges when necessary, but their everyday function, as sloped parklands and recreational areas for inhabitants of an especially gray and unpleasant part of an especially gray city, is equally or more important. Deployable walls, camouflaged as a series of murals that hang from strong hinges on the ugly underside of the FDR Drive, are another key part of the proposal. Most of the time, the structures, which will be designed by local artists, operate as decorative ceiling panels that enhance the experience of walking beneath the highway, which, lacking good alternatives, thousands of residents do each day. Occasionally they'll have other functions, such as blocking out wind and framing space for a protected seasonal food market. And when hurricanes hit, the walls flip down to become hard barriers, reducing the odds that floodwaters will devastate the area again.

Innovating communications infrastructure is increasingly part of the social infrastructure as well, particularly when it promotes face-to-face interaction or sustained dialog. But, as recent history has shown, social media can have a polarizing effect, particularly during elections and other pivotal political moments, solidifying bubbles and boundaries instead of weakening them. People can use digital media to find new friends and expand their horizons, but also to avoid the kind of intimate human contact that deep relationships and community-building requires. Today we are investing heavily in the communications infrastructure, but not in the kinds of social infrastructure that bring different people together "in real life." That's neither wise nor sustainable.

Different social infrastructures play distinct roles in the local environment, and support various kinds of social ties. Some places, such as libraries and schools, provide space for recurrent interaction, often programmed, and they tend to encourage thicker, more durable relationships. Others, such as playgrounds and street markets, tend to support thinner connections, but of course these ties can, and sometimes do, grow more substantial if the interactions become more frequent or the parties establish a deeper bond. Countless close friendships between mothers, and then entire families, began because two infants frequent

the same swing set. Basketball players who participate in regular pick-up games often befriend people with different political preferences, or with a different ethnic, religious, or class status, and wind up exposed to ideas they wouldn't otherwise confront off the court.

Some social infrastructures encourage in-group solidarity, while others, like public athletic fields and childcare centers, promote interaction across group lines. In elite American communities, private country clubs, some of which forbid female members and informally exclude certain ethnic or racial minorities, help build strong social bonds and business networks that ultimately deepen the nation's divisions and inequities. Border walls, including the one that currently separates parts of Israel and Palestine as well as the one that President Trump promises to build on the border of Mexico and the U.S., are quintessentially anti-social infrastructures. Paradoxically, zones around border walls, including checkpoints and access gates, often attract a diverse set of people, including members of the very groups that the structure is meant to separate, and occasionally they become sites for political engagement and protest. But their net impact is unmistakable: On good days, they segregate, discriminate, and entrench inequalities; on bad days, they incite violence.

The social infrastructure plays a critical but under-appreciated role in modern societies. It influences seemingly mundane but actually consequential practices and routines, from the way we move about our neighborhoods, schools, and commercial districts to the opportunities we have to casually interact with strangers, friends, and neighbors. It is especially important for children, the elderly, and other people whose limited mobility and lack of autonomy binds them to the places where they live. But the social infrastructure affects everyone, and determines our capacity to address the biggest challenges of our time, from social isolation and polarization to crime, education, health, and climate change.

The social infrastructure rarely crashes as completely or as visibly as a fallen bridge or downed electrical line, and its breakdowns don't result in immediate systemic failures. But when it's degraded the consequences are unmistakable. People reduce the time they spend in public settings and hunker down in their safe houses. Social networks weaken. Old and sick people grow isolated. Distrust rises and civic participation wanes.

We ignore it at our peril.

Appendix E

Solution Set: The Context

A well-functioning democratic system is built on an intricate web of rights and responsibilities between civil society and government. It requires, among other things, a citizenry that is informed, engaged, and committed to core democratic values. It relies on active debate and tolerance for dissent and opposing views, as well as a robust fourth estate.

Public Responsibilities	Mediating Norms and Institutions	Government Responsibilities
<p>Informed Citizenry through education and an impartial media.</p> <p>Engaged Citizenry that stays informed and participates in democratic institutions from public hearings to voting.</p> <p>Commitment to Democratic Norms and Values including tolerance for dissent, equality under the law, compromise, and the protection of minorities.</p> <p>Shared Sense of National Identity while respectful of individual and minority or communitarian identities and rights. There must be a common sense of belonging and participation in the national project.</p>	<p>Rule of Law and equality under it for the governing and the governed alike.</p> <p>Free Press that is impartial and held to high standards of integrity, including the formal fourth estate and citizen journalists.</p> <p>Civil Society including the private sector, private organizations, religious and educational institutions, and interest groups.</p> <p>Social Contract that provides an inclusive sense of opportunity in the form of an accessible, stable, and growing middle class.</p> <p>Trust defined by an ongoing sense of legitimacy and consent between the governed and the governing.</p>	<p>Democratic Accountability via electoral system, the rule of law, checks and balances, and responsiveness to public.</p> <p>Transparency defined by accessibility to citizenry and mediating institutions. In the digital age, this requires speed and simplicity.</p> <p>Fairness defined by equal representation of citizenry in public debate, as well as in provision of services, procurement, etc. Lack of fairness leads to corruption.</p> <p>Effective Delivery of Services including provision of public goods, national security and public safety, economic growth, and social stability.</p> <p>Data Integrity including personal identification, and record-keeping.</p>

Appendix F

List of Participants

Launch Event – Global Progress Summit

Montreal, Canada

September 14-15, 2016

Nicolas Berggruen, Chairman, Berggruen Institute
Matt Browne, Founder, Global Progress
Giuliano da Empoli, CEO, Volta
Chrystia Freeland, Minister of Foreign Affairs, Canada
Nathan Gardels, Senior Advisor, Berggruen Institute
Reid Hoffman, Founder & CEO, LinkedIn
Toomas Ilves, Former President of Estonia
Sadiq Khan, Mayor of London
Dawn Nakagawa, EVP, Berggruen Institute
Ben Rattray, Founder, Change.org
Alec Ross, Senior Advisor for Innovation, Hillary Rodham Clinton
Reshma Saujani, Founder, Girls Who Code
Eric Schmidt, Chairman, Alphabet
Justin Trudeau, Prime Minister of Canada

Roundtable Discussion I: Social Media and Cyber Security

New York, USA

December 15-16, 2016

Shaukat Aziz, Former Prime Minister of Pakistan
Nicolas Berggruen, Chairman, Berggruen Institute
Gordon Brown, Former Prime Minister of the United Kingdom
Fernando Henrique Cardoso, Former President of Brazil
Juan Luis Cebrian, Founding Editor in Chief, El País
María de Mar García, Philosopher & Spanish Politician
Kemal Dervis, Former Head of United Nations Development Program
Frank Fukuyama, Senior Fellow, Freeman Spogli Institute
Felipe Gonzalez, Former MOP, Spain
John Gray, Professor of European Thought, London School of Economics
Arianna Huffington, Founder, Huffington Post
D.T. Ignacio Jayanti, Managing Partner, Corsair
Vikram Jayanti, Documentary Filmmaker
Mickey Kantor, Former U.S. Secretary of Commerce
Pascal Lamy, Former Commissioner for Trade, E.U. Commission
Michael Lynton, Chairman, SnapChat
Kishore Mahbubani, Dean, Lee Kuan Yew School of Public Policy
Paul Martin, Former Prime Minister of Canada
Mario Monti, Former Prime Minister of Italy
David Muir, Journalist, ABC World News Tonight

Dawn Nakagawa, EVP, Berggruen Institute
Pierre Omidyar, Founder, Ebay
Raghuram Rajan, Governor, Reserve Bank of India
Dani Rodrik, Economist
Alec Ross, Senior Advisor for Innovation, Hillary Rodham Clinton
Nouriel Roubini, Co-Founder & Chairman, Roubini Global Economics
Robert Rubin, Chair, Council on Foreign Relations
Anya Schiffrin, Director of Technology, Media & Communications, Columbia University
Eric Schmidt, Chairman, Alphabet
Stephen Schwarzman, Chairman & CEO, The Blackstone Group
Evan Spiegel, Founder & CEO, SnapChat
Joe Stiglitz, Nobel Laureate, Economics
Larry Summers, Former Director of the National Economic Council
Helle Thorning-Schmidt, CEO, Save the Children International
Feng Wei, Secretary General, Institute for Innovation & Development Strategy
Jerry Yang, Co-founder & Former CEO, Yahoo
George Yeo, Former Minister of Foreign Affairs, Singapore
Fareed Zakaria, Host, CNN
Ernesto Zedillo, Former President of Mexico

Round Table Discussion II: Renovating Democracy

Lisbon, Portugal

April 16-17, 2017

Asaf Akat, Economist
Matt Browne, Founder, Global Progress
Juan Luis Cebrian, Founding Editor in Chief, El País
Jim Fishkin, Chair, International Communication, Stanford University
Nathan Gardels, Senior Advisor, Berggruen Institute
Nilufer Gole, Sociologist
Fernando Henrique Cardoso, Former President of Brazil
Ernesto Ottone, President, National Council for Culture & the Arts
Pascal Perinneau, Professor, Sciences Po
Marcelo Rebelo de Sousa, President of Portugal
Alain Touraine, Research Director, École des Hautes Études en Sciences Sociales
Michel Wieviorka, Sociologist

Roundtable Discussion III: Managing Fake News

Menlo Park, USA

May 3-4, 2017

Nicolas Berggruen, Chairman, Berggruen Institute
Emily Bell, Founding Director, Tow Center for Digital Journalism
Matt Browne, Founder, Global Progress
Campbell Brown, Head of New Partnerships, Facebook
Larry Diamond, Senior Fellow, Hoover Institute

Eileen Donahoe, Executive Director, Global Digital Policy Incubator
Jack Dorsey, Founder & CEO, Twitter
Frank Fukuyama, Senior Fellow, Freeman Spogli Institute
Nathan Gardels, Senior Advisor, Berggruen Institute
Wael Ghonim, Internet Activist / Product Manager, Quora
Peter Gloor, Research Scientist, Center for Collective Intelligence
Reid Hoffman, Founder, LinkedIn
Toomas Ilves, Former President of Estonia
Jerry Kaplan, Entrepreneur, Stanford University
Margaret Levi, Director, Center for Advanced Study of Behavioral Science
Leslie Miller, Government Affairs, Google
Dawn Nakagawa, EVP, Berggruen Institute
Ariel Ratner, Founder & CEO, Inside Revolution
Ben Rattray, Founder, Change.org
Peter Schwartz, Senior Vice President, Salesforce.com
Jeff Skoll, Founder, Skoll Foundation
Patrick Soon Shiong, Founder & CEO, NantWorks
Ola Tjornbo, Principal, Archipelago Consultants
Jerry Yang, Co-founder & Former CEO, Yahoo

Roundtable Discussion IV: Renovating Democracy
Washington DC, USA
June 26, 2017

Kristen Anderson, Host, The Pollsters
Robert Atkinson, President, Information Technology & Innovation Foundation
John Borthwick, CEO, Betaworks
Matt Browne, Founder, Global Progress Summit
Amy Dacey, Executive Vice President, MWWPR
Wael Ghonim, Internet Activist / Product Manager, Quora
Vinny Green, Vice President, Snopes
Sarah Hurwitz, Former Speechwriter, White House
Toomas Ilves, Former President of Estonia
Rose Jackson, Senior Policy Advisor, Open Society Foundation
Lorelei Kelly, Fellow & Director, Beeck Center for Social Impact and Innovation
Karen Kornbluh, Senior Fellow for Digital Policy, Council on Foreign Relations
Kaj Larsen, Senior Correspondent, NowThis
Thomas Malone, Founding Director, Center for Collective Intelligence
Martin Moore, Director, Centre for the Study of Media, Communication & Power
Caroline Mauldin, Executive Director, South Carolina Future Minds
Dawn Nakagawa, EVP, Berggruen Institute
Bill Nichols, Vice President, Freedman Consulting
Ola Tjornbo, Principal, Archipelago Consulting
Thomas Pitfield, President, Canada 2020
Ariel Ratner, Founder & CEO, Inside Revolution
Alec Ross, Democratic Candidate, Governor of Maryland
Jody Sadornas, Program Manager, Berggruen Institute

Seth Stodder, Former U.S. Assistant Secretary of Homeland Security
Devinda Subasinghe, Former Sri Lankan Ambassador to the United States
Andrew Wilson, President, Center for International Private Enterprise