Hastings Law Journal

Volume 69 | Issue 5 Article 3

6-2018

Can Democracy Withstand the Cyber Age?: 1984 in the 21st Century

David M. Howard

Can Democracy Withstand the Cyber Age?: 1984 in the 21st Century

DAVID M. HOWARD*

Democracy has evolved throughout history, and democracy can survive the challenges of the cyber age. However, democracy will be affected by the internet and increased cybersecurity. Cybersecurity and democracy sometimes appear at odds, and the recent cyberattacks on democratic elections show the growing need for strengthened cybersecurity. Yet these efforts to increase cybersecurity must comport with the needs of democracy. This Article describes the potential conflicts between cybersecurity and the foundations of democracy, and argues that for democracy to survive the coming decades, cybersecurity efforts must support the values that sustain our democracy, particularly that of free speech and informed voting. While we are in a dangerous period of modern history, this Article further argues that the requirements of cybersecurity and democracy do not need to be mutually exclusive, but that the internet can enhance democratic institutions.

* Associate at Baker Botts L.L.P. in New York, NY., J.D., University of Texas School of Law, 2017. The opinions expressed herein are the Author's own and do not necessarily reflect those of Baker Botts L.L.P. This Article is dedicated to his loving and incredibly supportive wife, Jingjing Liang, who listens to him talk about his legal theories quite often. The Author would like to thank Dean Lawrence G. Sager for his support, encouragement, and mentorship. The Author would also like to thank Professor Philip Bobbitt for his advice and assistance in forming this piece and the book project that will come from this Article.

TABLE OF CONTENTS

INTRODUCTION

By now, the Russian interference in the 2016 U.S. presidential election, which many have called a direct attack on democracy, has been discussed throughout the world.[1] This is not the only recent attack on a democracy. Within the last year alone, hackers of foreign governments have injected themselves into the 2017 French election of Emmanuel Macron,[2] the 2017 German election of Angela Merkel,[3] and likely even into the referendum vote for Catalonian independence,[4] resulting in what has been named a new "social media blitzkrieg."[5] This growing trend of attempts by outside actors to influence democratic elections provides a dark and somewhat ominous tone for the future of democracy in our world. Yet, there is still a bright silver lining to this seemingly dangerous period in modern democratic history.

---

1. *See, e.g.*, *Russia Aims to Meddle in State Elections, Sen. King Says*, NPR (June 21, 2017, 7:38 AM), http://www.npr.org/2017/06/21/533774626/russia-aims-to-meddle-in-state-elections-sen-king-says.

2. Alex Hern, *Macron Hackers Linked to Russian-affiliated Group Behind US Attack*, GUARDIAN (May 8, 2017), https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

3. Constanze Stelzenmüller, *The Impact of Russian Interference on Germany's 2017 Elections*, BROOKINGS INST. (June 28, 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

4. Natasha Bertrand, *Julian Assange Is Rallying Behind Catalan Separatists Ahead of a Historic Referendum—and Russia Has Taken Notice*, BUS. INSIDER (Sept. 30, 2017, 2:10 PM), http://www.businessinsider.com/julian-assange-catalonia-independence-movement-and-referendum-spain-2017-9.

5. Max Boot, *Russia Has Invented Social Media Blitzkrieg*, FOREIGN POL'Y (Oct. 13, 2017, 9:00 AM), http://foreignpolicy.com/2017/10/13/russia-has-invented-social-media-blitzkrieg/.

Democracy can survive the cyber age. However, democracy will be affected by the internet and cybersecurity. The rise of the internet has significantly altered how people live, particularly the methods used to obtain information and communicate with others. The internet is a new landscape where information is disseminated rapidly and wars are increasingly fought. These new channels of communication and international connection have created a need for cybersecurity to protect states from new types of warfare and espionage. For many states, this has included monitoring people and gathering information on their own citizens. These emerging factors, as discussed in this Article, affect the very foundation of democracy.

Scholars have been fascinated by this issue since the internet became more prevalent, but many continue to disagree on the effects the internet will have on democracy.[6] This Article is written partly in response to scholars, particularly Professor Nathaniel Persily, who posit a very relevant and essential question for this country: whether democracy can survive the internet. Focused on the 2016 U.S. presidential election, Professor Persily's recent Article leaves us with a chilling conclusion: that democracy is already deteriorating and we should not expect technology to rescue us from these threats to democracy.[7]

I agree with Professor Persily's assumption that democracy depends on voters' ability to be informed of relevant facts upon which to base their political judgments and I do not dispute the discussion of events surrounding the 2016 presidential election. However, I disagree with the fundamental conclusion that democracy is deteriorating, at least with regard to the notion that the internet is the cause and that technology cannot be the solution. The rise of the internet and the resulting cybersecurity measures will not destroy democracy; rather it will change democracy.

This Article discusses the definition of democracy and how the definition will change with the increased use of the internet and technology. While the internet is currently one of the mediums altering the foundations of democracy, technology can also be the very system to strengthen democracy in its shifting form if that technology is used

6. *See, e.g.*, Dan Hunter, *ICANN and the Concept of Democratic Deficit*, 36 LOY. L. A. L. REV. 1149, 1152 (2003); Rachel Kerestes, *The Web of Politics: The Internet's Impact on the American Political System*, 6 GEO. PUB. POL'Y REV. 89, 89 (2000) (book review).

7. Nathaniel Persily, *Can Democracy Survive the Internet?*, 28 J. DEMOCRACY 63, 74–75 (2017) ("With the deterioration in democratic values occurring both on- and offline, we should not expect technology to rescue us from the historical and sociological forces currently threatening democracy, even if that same technology facilitated the disruption in democratic governance in the first instance.").

correctly. Part I of this Article discusses the definition of democracy and focuses on the two pillars commonly found in most definitions, freedom of speech and informed voting. Part II and III discuss how the internet affects these two pillars of democracy and focuses on a few examples, including the Russian interference in the 2016 U.S. election and the spread of false information throughout the world. Finally, Part IV concludes the Article.

I. DEMOCRACY AND CYBERSECURITY

The internet will not destroy democracy, though it will change it. To understand the arguments, this Article must first define "democracy" and "cybersecurity" because their definitions are co-dependent. The first part of this discussion defines these terms and identifies the principles involved.

Democracy is fairly adaptable to shifting circumstances,[8] and this form of government has lasted in substantially similar forms since at least the ancient Greeks.[9] Long before the United States was founded, many, including scholars and politicians, have attempted to create an overarching definition of democracy. The definition of democracy is broad enough to allow changes in its structure, and democracy responds as changes arise. Countries have changed their political structures significantly throughout history, moved by changing technology and pushed along by evolving warfare.[10] As the political foundations for states alter, a nation based on democracy also alters its fundamental structure.[11] To respond to these changes in our political system, it is necessary to understand how technology will change democracy.

Much has been written about democracy as a theory and the principles this ideal does and should embody. Aristotle supposedly defined democracy as: "any regime in which the 'people' (dēmos) rule or control the authoritative institutions of the city; more properly, rule of the poor or the majority in their own interest."[12] Robert Dahl characterized democracy as "the freedom of self-determination in making collective and binding decisions: the self-determination of citizens entitled to participate as political equals in making the laws and

8. COUNCIL OF EUROPE, REFLECTIONS ON THE FUTURE OF DEMOCRACY IN EUROPE 21 (2005).

9. Jeffrey Usman, *Non-Justiciable Directive Principles: A Constitutional Design Defect*, 15 MICH. ST. J. INTL'L L. 643, 655-56 (2007).

10. *See generally* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY (2002) (describing the historical change in the foundations of states from the time of the "princely" state to the current "market" state, developing in part to shifting needs and circumstances of the peoples).

11. Gary C. Leedes, *The Latest and Best Word on Legal Hermeneutics: A Review Essay of* Interpreting Law and Literature: A Hermeneutic Reader, 65 NOTRE DAME L. REV. 375, 393 (1990).

12. ARISTOTLE, THE POLITICS 275 (Carnes Lord trans., 1984).

rules under which they will live together as citizens."[13] Ronald Dworkin defined democracy as a form of government where:

> the citizens of a political community govern themselves, in a special but valuable sense of self-government, when political action is appropriately seen as collective action by a partnership in which all citizens participate as free and equal partners, rather than as a contest for political power between groups of citizens.[14]

While these are only a representative sample of the varying definitions of democracy, the underlying principles remain the same. "Democracy" as an ideal refers to "rule by people," and a desire for this ideal has never been greater.[15] To this end, modern democratic governance generally denotes several foundations: effective participation of its citizens (including freedom of speech), voting equality for its people, rule of law, separation of powers, and individual rights.[16] Modern democracy is a system of governance in which leaders are accountable for their actions to their citizens through the citizens' representatives.[17]

This Article focuses on two of the most relevant, and arguably the most fundamental, foundations of modern democracy: (1) freedom of speech and (2) informed voting. Freedom of speech provides vigorous debate and dissemination of various ideas and prevents a state from controlling the thoughts and minds of its people through enforced silence or censorship.[18] Freedom of speech is essential to effective participation of citizens in governance and is required by democracy in general.[19] In the United States, the First Amendment was designed to protect democracy[20] and free speech is essential to that democracy.[21] If one looks to the new subtitle of the Washington Post, it reads: "Democracy

13. ROBERT A. DAHL, DEMOCRACY AND ITS CRITICS 326 (1989).

14. Ronald Dworkin, *The Partnership Conception of Democracy*, 86 CALIF. L. REV. 453, 453 (1998).

15. Philippe C. Schmitter, *Crisis and Transition, but Not Decline*, *in* DEMOCRACY IN DECLINE 39, 39 (Larry Diamond & Marc F. Plattner eds., 2015); Senator Bob Dole, *Foreword*, 35 HARV. J. ON LEGIS. 1, 1 (1998) ("The result is a world order far smaller, faster, and more democratic than could have been imagined just a decade ago.").

16. Same Varayudej, *A Right to Democracy in International Law: Its Implications for Asia*, 12 ANN. SURV. INT'L & COMP. L. 1, 17 (2006).

17. Molly Beutz, *Functional Democracy: Responding to Failures of Accountability*, 44 HARV. INT'L L.J. 387, 401 (2003); Philippe C. Schmitter & Terry Lynn Karl, *What Democracy Is . . . and Is Not*, 2 J. DEMOCRACY 75, 76 (1991); PAUL WOODRUFF, FIRST DEMOCRACY: THE CHALLENGE OF AN ANCIENT IDEA ix (2005).

18. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339 (2010) ("Speech is an essential mechanism of democracy, for it is the means to hold officials accountable to the people.").

19. RONALD DWORKIN, JUSTICE FOR HEDGEHOGS 4 (2011).

20. Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of Youtube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319, 369 (2012).

21. Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 34 (2004).

dies in darkness."[22] This could not be more accurate in the context of free speech.[23]

The second pillar—informed voting—may be the most vital requirement of democracy. Only a citizenry with access to truthful and accurate information necessary to make a beneficial decision can enact the most operative laws or elect the most effective representatives.[24]

Through informed voting, citizens can hold their representatives accountable to the needs of the people.[25] Our democracy requires the right to vote and the right to access and send information to others. The U.S. Constitution protects both of these rights and these rights are arguably the most vigorously debated and litigated rights in our political and judicial systems. Other rights are affected by the rise of the internet and cybersecurity, but this Article will focus on the two described above.

Like the printing press in the late eighteenth century and the newspapers and radio stations of the twentieth century, the internet is the greatest tool for communication today.[26] The internet is our primary source of news, information, and ideas. It has become the core infrastructure of modern free expression and speech, and the internet is often considered the basis for twenty-first century society.[27] Developments in electronic communication have opened new channels of access outside of the traditional media sources.

The argument laid out in this Article applies to democracy generally throughout the world, but particularly in the United States. While some have argued the United States is a republic rather than a democracy, this argument fails to consider the overlap between the two forms of governance. A "republic" is often defined as "a government in which supreme power resides in a body of citizens entitled to vote and is exercised by elected officers and representatives responsible to them and governing according to law."[28] The United States fits this description. As discussed above, "democracy" is defined in a similar manner, yet democracy has several varying forms, such as a pure or direct democracy

22. *The Washington Post*, WASH. POST, https://www.washingtonpost.com (last visited May 7, 2018).

23. *See* Michael C. Shaughnessy, *Praising the Enemy: Could the United States Criminalize the Glorification of Terror Under an Act Similar to the United Kingdom's Terrorism Act 2006?*, 113 PENN. ST. L. REV. 923, 981 (2009) ("Free speech can survive without the United States, but the United States cannot survive without free speech.").

24. *See* McCutcheon v. Fed. Election Comm'n, 134 S. Ct. 1434, 1440–41 (2014) ("There is no right more basic in our democracy than the right to participate in electing our political leaders.").

25. James A. Gardner, *Anti-Regulatory Absolutism in the Campaign Arena:* Citizens United *and the Implied Slippery Slope*, 20 CORNELL J.L. & PUB. POL'Y 673, 698 (2011).

26. Sascha Meinrath & Marvin Ammori, *Internet Freedom and the Role of an Informed Citizenry at the Dawn of the Information Age*, 26 EMORY INT'L L. REV. 921, 922 (2012).

27. *Id.*

28. *Republic*, MERRIUM-WEBSTER'S NEW AMERICAN DICTIONARY (3d. ed. 1993).

where citizens have direct participation in decisionmaking rather than through representatives.[29] The United States fits the above description of democracy as well.[30] So when discussing the form of governance in this country, the answer to "which form is the United States?" is technically "both." Rather than a direct or pure democracy, the United States is more of a representative and constitutional democracy.[31] This Article will focus on the democratic aspects of a state, including that of the United States.

For simplicity's sake, this Article will use a broad definition of democracy in an attempt to encompass the commonalities between the definitions discussed above: "Democracy is a system of governance where the power to govern derives from the governed."[32] That power comes from democratic values, including free speech and informed voting. Because the argument in this Article is largely based on the definition of democracy, the use of a broad definition seeks to cover as many issues and arguments as possible regarding the effect of cybersecurity on democratic governance. The attempt of this Article is not to create an additional definition for democracy, but to oppose the idea that the internet and cybersecurity are destroying democracy. We must understand the meaning of democracy, otherwise this discussion cannot take place.[33]

II. CYBERSECURITY WILL CHANGE THE FOUNDATION OF DEMOCRACY

Even though it is almost universally agreed that increased cybersecurity is necessary to protect the functions of the state from cyberattacks, there is less agreement on what cybersecurity actually entails.[34] Cyber-war might be most frequently defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[35] For the purposes of this discussion, "cybersecurity" means "protecting the basic security of computerized systems from unauthorized access."[36]

---

29. Theo Schiller, *Direct democracy*, BRITANNICA, https://www.britannica.com/topic/direct-democracy (last visited May 7, 2018).

30. Maureen B. Cavanaugh, *Democracy, Equality, and Taxes*, 54 ALA. L. REV. 415, 438 (2003).

31. Erwin Chemerinsky, *A Grand Theory of Constitutional Law?*, 100 MICH. L. REV. 1249, 1256 (2002) ("Neither descriptively nor normatively is majority rule a proper definition of American democracy.").

32. THE DECLARATION OF INDEPENDENCE (U.S. 1776).

33. DWORKIN, *supra* note 19, at 6.

34. Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 587 (2011).

35. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010).

36. Jeffrey F. Addicott, *Enhancing Cybersecurity in the Private Sector by Means of Civil Liberty Lawsuits—the Connie Francis Effect*, 51 U. RICH. L. REV. 857, 875 (2017).

Cybersecurity is a necessary response to cyberattacks and cyberwarfare.[37] But cyberattacks are not simply hacking information, monitoring people, altering news, or interfering with electronic voting; they can have other consequences as well, including physical. There are generally four categories of actors in cyberattacks: terrorists, nation-states, terrorist sympathizers, and thrill seekers.[38] Cyberattacks are often broken down into four general categories: criminal activity, espionage, terrorism, and cyberwarfare, although many actors have more than one motive.[39]

The rise of cyberattacks is not a recent phenomenon. In 1982 during the Cold War, a pipeline in Soviet Siberia exploded due to U.S. efforts to infiltrate Soviet information system.[40] The United States, in collaboration with Israel, used cyberattacks including the Stuxnet code to halt nuclear processes in Iran.[41] In 2007, the communication and banking systems of Estonia were taken down by cyberattacks throughout the country.[42] A Canadian hacker recently admitted that Russian government agents hired him to break into Yahoo's systems and steal personal information of Yahoo users.[43] In 2017, Equifax was hacked, losing millions of American citizen's personal information.[44] Cyberattacks are one of the newest evolving weapons, and it seems as if this weapon is only now being exploited to its full potential. This results in many problems, such as a threefold increase in cyberattacks on private companies' internet systems.[45] In fact, a U.K. terror reinsurer recently began offering coverage against cyberattacks in response to this rise.[46]

---

37. *See* Bambauer, *supra* note 34, at 587.

38. Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 404 (2007).

39. Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1278 (2013).

40. David E. Hoffman, *Reagan Approved Plan to Sabotage Soviets*, WASH. POST (Feb. 27, 2004), https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/?utm_term=.4c03ad57aee0.

41. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A21.

42. Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2017), http://www.bbc.com/news/39655415.

43. *Yahoo 'Hacker-for-Hire' Pleads Guilty*, BBC NEWS (Nov. 29, 2017), http://www.bbc.com/news/technology-42166088.

44. Tara Siegel Bernard et al., *Equifax Attack Exposes Data of 143 Million in the U.S.*, N.Y. TIMES, Sept. 8, 2017, at A1.

45. Reuters Staff, *German Companies See Threefold Rise in Cyber Attacks, Study Finds*, REUTERS (Oct. 5, 2017, 8:25 AM), https://www.reuters.com/article/us-cyber-attack-germany/german-companies-see-threefold-rise-in-cyber-attacks-study-finds-idUSKBN1CA1WX.

46. William Shaw, *UK Terror Reinsurer to Start Offering Cyberattack Cover*, LAW360 (Nov. 28, 2017, 12:50 PM), https://www.law360.com/cybersecurity-privacy/articles/988691/uk-terror-reinsurer-to-start-offering-cyberattack-cover.

New weapon technology, including cyber technology, pushes policy, guides politics, and changes the course of history.[47] In addition to causing physical and technological problems, cyberattacks can impact psychology by, for example, spreading of false information. Yet planting inaccurate information is not only useful to adversaries in military operations, it can also be used to affect civilian thought. New social media platforms and technology have become useful tools for cyberattacks, where politics can be influenced and populations bombarded with information both true or false: essentially becoming a "weapon of mass disruption."[48] Democracy relies on accurate information to support informed voting, and hackers have taken advantage of this fact. The same way that governments or news companies can use social media to spread relevant news and promote free speech, so can terrorists and other state or non-state actors use it for disinformation campaigns and recruiting others to their causes.[49]

The rise of social media and access to the internet permits these problems. During the Cold War, countries attempted to spread disinformation in other countries, but it was more difficult than it is now.[50] With the rise of the cyber age, anyone can get information through a growing number of internet sources, including sources that are not vetted through the traditional and more transparent media forms.[51] Even the appearance of disinformation or outside intervention in democratic elections can affect confidence in the media, causing many to no longer trust the sources that provide the news they receive.[52] Trust in the media has recently dropped, especially after reports were released detailing the Russian use of false Twitter accounts to influence political views in the United States.[53] Democracy depends on the people's faith that our

47. *See* BOBBITT, *supra* note 10, at 13-16 (describing the advances in weapon technology that changed the strategies and relations of international powers).

48. BILL GERTZ, IWAR: WAR AND PEACE IN THE INFORMATION AGE 35 (2017).

49. Press Release, The White House, Office of the Press Secretary, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015).

50. Neil MacFarquhar, *Russia's Powerful Weapon to Hurt Rivals: Faslehoods*, N.Y. TIMES, Aug. 29, 2016, at A1.

51. Samantha Power, Opinion, *Samantha Power: Why Foreign Propaganda Is More Dangerous Now*, N.Y. TIMES (Sept. 19, 2017), https://www.nytimes.com/2017/09/19/opinion/samantha-power-propaganda-fake-news.html.

52. Clint Watts, *Why Russia Wants the U.S. to Believe the Election Was Hacked*, PBS: NOVA (Oct. 26, 2016), http://www.pbs.org/wgbh/nova/next/tech/election-cybersecurity/.

53. *See* Olivia Beavers, *Twitter Account Claiming to Belong to Tennessee GOP Was Run by Russian Trolls*, THE HILL (Oct. 18, 2017, 3:04 PM), http://thehill.com/policy/cybersecurity/356066-popular-twitter-account-claiming-to-belong-to-tennessee-gop-was-run-by.

governmental structure can accommodate this social change,[54] and this faith is currently under attack.

Counter to the informed position of several scholars, including Professor Nathaniel Persily, democracy will not fall because of the internet; instead democracy will adapt and even strengthen through the age of the internet. Admittedly, democracy has and will continue to have problems, particularly in emerging states.[55] Throughout history, democracies and their laws have not kept pace with advances in technology.[56] While I do not agree with the notion that democracy around the world is in decline as some scholars do,[57] this Article simply argues that the internet and cybersecurity is not the driving cause. Rather, if handled properly, the internet, particularly social media, can enhance democratic values rather than destroy them. Technology has advanced faster than countries can keep up. Democracy has faced many challenges, and this is just the newest hurdle we must overcome.

States must balance many interests in this pursuit of strengthening democracy. Most importantly, states must balance the interest of national security against an interest in free speech. Much of the advances in social media allow people to increase their ability to speak at levels never seen before, but these same advances permit activities such as hacking, information warfare, and cyber terrorism. How far can democracies regulate or prohibit these technological advances without limiting or destroying either free speech, free dissemination of information, or our fundamental pillars of democracy? This is, and will continue to be, the essential question for this generation. How we answer this question will affect democracy itself: move too far to protect national security and we lose our democratic foundations; overprotect speech and we lose the ability to defend countries from cyberattacks and foreign interference. Informed voting deals with the same problem: balancing national security interests against the need to disseminate information necessary to allow voters to make educated decisions. These two pillars overlap in many respects, but can be affected by the internet in different ways.

---

54. Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 244 (2011).

55. *See generally* DEMOCRACY IN DECLINE? (Larry Diamond & Marc F. Plattner eds., 2015) (arguing that democracy in emerging states faces many difficulties, even today).

56. Christopher R. Orr, *Your Digital Leash: The Interaction Between Cell Phone-Based GPS Technology and Privacy Rights in* United States v. Skinner, 45 U. TOL. L. REV. 377, 401 (2014).

57. *See, e.g.*, Larry Diamond, *Facing Up to the Democratic Recession*, *in* DEMOCRACY IN DECLINE? 98 (Larry Diamond & Marc F. Plattner eds., 2015); John Braithwaite, *Criminal Justice That Revives Republican Democracy*, 111 NW. U. L. REV. 1507, 1510 (2017) (arguing that "democracy engenders money politics and thereby drives up domination, destroying the very freedom of citizens that is democracy's rationale").

III. CYBERATTACKS AFFECT THE FOUNDATIONS OF DEMOCRACY

The internet comes with problems, just as democracy does.[58] This next challenge—particularly foreign interference in democratic elections through the spread of false information—will be one of the hardest challenges democracy has faced. Countries have interfered in foreign democratic elections throughout history, even after World War II and the Cold War, and this interference continues today.[59] China, Russia, and the United States (among others) have all either coerced, or outright interfered in, foreign elections, with the 2016 U.S. presidential election as an example of the most recent type of intrusion.[60] Outside interference in democratic elections through cyber channels even appeared in the recent 2017 Catalonian vote for independence.[61] But the volume and widespread methods of the recent interference by foreign governments into democratic elections appears to be generally unprecedented: sending disinformation directly to voters through the internet and attempting to hack voter registries and voting machines.

A. TYPES OF CYBERATTACKS

As described above, there are two broad types of actors in cyberattacks: government and private actors. Private actors are further classified into categories based on the attack's purpose: criminal, terrorist, or (h)acktivists. Cybercrime, including spam-ware and malware, spans a broad set of actions used in attempts to either obtain private information[62] or extort money from individuals or companies (often referred to as ransomware).[63] Hackers recently used ransomware attacks on several entities, including the law firm DLA Piper,[64] and the

58. *See generally* CHRISTOPHER H. ACHEN & LARRY M. BARTELS, DEMOCRACY FOR REALISTS: WHY ELECTIONS DO NOT PRODUCE RESPONSIVE GOVERNMENT (2016) (asserting that democracy does not necessarily produce responsive governments because voters mostly choose parties and candidates on the basis of social identities and partisan loyalties, not political issues).

59. Lily Rothman, *Fear of Foreign Intervention in U.S. Politics Goes Back to the Founding Fathers*, TIME (Dec. 17, 2016), http://time.com/4604464/foreign-interference-history/.

60. *Id.*

61. Dan Boylan, *Russian Interference Seen in Catalonia Crisis, Security Experts Say*, WASH. TIMES (Oct. 2, 2017), https://www.washingtontimes.com/news/2017/oct/2/russian-interference-seen-catalonia-crisis/.

62. Lee Mathews, *Email Spam Surges to Highest Level in More Than Two Years*, FORBES (Aug. 8, 2017, 11:48 AM), https://www.forbes.com/sites/leemathews/2017/08/08/email-spam-surges-to-highest-level-in-more-than-two-years/#51a154b6e304.

63. Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DISCOURSE 320, 329 (2016) (defining ransomware as "malicious software that encrypts a computer's hard drive and renders the information on it permanently inaccessible unless the victim pays the attackers (often in Bitcoin) to restore access").

64. Barney Thompson, *DLA Piper Still Struggling with Petya Cyber Attack*, FIN. TIMES (July 6, 2017), https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.

England's NHS trusts.[65] By shutting down the computer system of a large company or government, hackers can effectively paralyze their systems.[66] Hacktivists are also a growing phenomenon, with groups such as Anonymous or Lulz Security using cyberattacks or cybercrime in attempts to influence policy or make political statements.[67]

Cyberattacks by governments have become increasingly publicized and are a growing concern, especially after the 2016 U.S. presidential election. Cyberattacks by foreign governments in democratic elections pose a grave threat to the democratic process.[68] Generally, governments (foreign or domestic) can interfere in democratic elections through (1) manipulating facts and opinions that inform how citizens vote, (2) interfering with the act of voting (for example, tampering with voter registration polls), (3) changing the vote results, and (4) undermining confidence in the integrity of the vote.[69] Russian cyberattack interference in, for example, Estonia's government, political parties, and banks, inhibited internet usage for two weeks.[70] In 2009, a DDoS attack targeted U.S. and South Korean government websites, which some experts believe originated from either China or North Korea.[71]

Cyberattacks can also be used by terrorist organizations. ISIS frequently uses the internet to recruit new members and spread propaganda, but the internet creates the potential for ISIS to use cyberattacks against foreign governments.[72] For example, hackers linked to ISIS posted online the personal information of over 3000 people, along with death threats.[73] While this type of cyberattack has not been a large part of their campaigns, it has the potential to become a new arena for terrorist organizations. With the loss of ISIS's physical territory, some

65. *NHS 'Could Have Prevented' WannaCry Ransomware Attack*, BBC NEWS (Oct. 27, 2017), http://www.bbc.com/news/technology-41753022.

66. Olivia Solon & Alex Hern, *'Petya' Ransomware Attack: What Is It and How Can It Be Stopped?*, GUARDIAN (June 28, 2017, 2:17 PM), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

67. Swathi Padmanabhan, *Hacking for Lulz: Employing Expert Hackers to Combat Cyber Terrorism*, 15 VAND. J. ENT. & TECH. L. 191, 198 (2012).

68. Anthony J. Gaughan, *Ramshackle Federalism: America's Archaic and Dysfunctional Presidential Election System*, 85 FORDHAM L. REV. 1021, 1033–34 (2016).

69. JAKOB BUND, CYBERSECURITY AND DEMOCRACY: HACKING, LEAKING, AND VOTING 3 (2016); TED PICCONE, DEMOCRACY AND CYBERSECURITY 2 (2017).

70. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 22 (2010).

71. Gabriel K. Park, *Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack*, 38 BROOK. J. INT'L L. 797, 803 (2013).

72. Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 390 (2011).

73. Jonathan Dienst et al., *ISIS-Linked Hackers Target 3,000 New Yorkers in Cyberattack: Officials*, NBC NEW YORK (Apr. 28, 2016, 7:49 PM), https://www.nbcnewyork.com/news/local ISIS-Linked-Hackers-Target-New-Yorkers-Personal-Information-377511431.html.

believe the terrorist organization may increase its online presence through cyberattacks.[74]

With the rise of cyberattacks, governments have increased cybersecurity. This natural reaction of the government is to protect its infrastructure and its citizens from these cyberattacks, but this reaction can result in a potentially larger problem than cyberattacks—government over-surveillance.

B. GOVERNMENT [OVER-]SURVEILLANCE AND CENSORSHIP HARMS DEMOCRACY

One of the most pressing issues in cybersecurity is not just foreign or independent interferences. Rather, of great importance is the ability of governments to observe, monitor, and even censor its own citizens, as this poses a grave threat to citizen's freedom of speech.[75] In the name of national security, many governments have increased their cybersecurity efforts, which often includes the monitoring of their own people.[76] When the government demanded access to user data, the CEO of Apple perfectly worded this tension of governmental intrusion into citizens' privacy: "[T]his demand would undermine the very freedoms and liberty our government is meant to protect."[77] Yet, while governmental intrusion into a citizen's own private life undermines many fundamental liberties, cybersecurity is a necessary component to protect a state from cyberattacks.[78] Cybersecurity requires regulation—specifically, regulation of the internet and its related tools.[79] Regulation of the internet is inherently regulation of communications, and with the integration of modern technology pervading virtually all of our activities, this type of regulation has the ability to monitor and affect virtually every aspect of our lives. Government regulation of the internet includes

74. David P. Fidler, *Terrorism, the Internet, and the Islamic State's Defeat: It's over, but It's Not over*, COUNCIL ON FOREIGN REL. (Nov. 28, 2017), https://www.cfr.org/blog/terrorism-internet-and-islamic-states-defeat-its-over-its-not-over.

75. *See* Alexandra Paslawsky, Note, *The Growth of Social Media Norms and Governments' Attempts at Regulation*, 35 FORDHAM INT'L L.J. 1485, 1539 (2012) ("Government intervention [in the internet] poses a greater threat to free speech than private action.").

76. Lee Rainie & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

77. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/.

78. David P. Fidler, *Transforming Election Cybersecurity*, COUNCIL ON FOREIGN REL. (May 17, 2017), https://www.cfr.org/report/transforming-election-cybersecurity.

79. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) ("This new boundary defines a distinct Cyberspace that needs and can create its own law and legal institutions."); Daniel J. Ryan et al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1195 (2011).

government surveillance of the internet. Excessive surveillance by government bodies can result in a chilling effect on how people live their lives.[80] One such example of this excessive monitoring is the attempt by the government to obtain access to constant cell-location data of individuals.[81] For example, the current U.S. Administration requested IP addresses of visitors to an anti-Trump website, which could be used to identify people who used the site to express their political ideas, something that "should be enough to set alarm bells off in anyone's mind."[82] The police have also used location data from Facebook and other social media sites to monitor and track protestors.[83]

Freedom of speech has different limits in each country, and its protections vary greatly even among democracies.[84] For example, although the United States adopted much of the legal system from Great Britain, the United States and United Kingdom have very different protections for speech.[85] Despite the differences in free speech protections, the U.K. is still a (parliamentary) democracy. Even so, cybersecurity measures deeply affect the protections of speech in democracies overall, and under the guise of national security, states often increase surveillance of the internet and their own citizens.[86]

In these situations, cybersecurity creates a deep chilling effect on speech. Governments who use claims of national security as a basis to monitor their citizens create a downward, self-propelling spiral: more cybersecurity means less free speech for fear of governmental intrusion while self-censorship of political views leads to less speech against that increased governmental surveillance. With the increase of reports about U.S. governmental surveillance of the internet, "Americans have altered

80. Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 161 (2016).

81. Lydia Wheeler, *Supreme Court Pressed to Rule on Police Access to Cellphone Data*, THE HILL (Aug. 31, 2015, 4:00 PM), http://thehill.com/regulation/court-battles/252357-supreme-court-urged-to-hear-case-over-access-to-cell-phone-records.

82. Morgan Chalfant, *Justice Demands 1.3M IP Addresses Related to Trump Resistance Site*, THE HILL (Aug. 14, 2017, 5:58 PM), http://thehill.com/policy/cybersecurity/346544-dreamhost-claims-doj-requesting-info-on-visitors-to-anti-trump-website.

83. Kristina Cooke, *U.S. Police Used Facebook, Twitter Data to Track Protesters: ACLU*, REUTERS (Oct. 11, 2016, 1:40 PM), https://www.reuters.com/article/us-social-media-data/u-s-police-used-facebook-twitter-data-to-track-protesters-aclu-idUSKCN12B2L7.

84. *See* Alex Gray, *Freedom of Speech: Which Country Has the Most?*, WORLD ECON. F. (Nov. 8, 2016), https://www.weforum.org/agenda/2016/11/freedom-of-speech-country-comparison/.

85. Ellen Parker, *Implementation of the UK Terrorism Act 2006—The Relationship Between Counterterrorism Law, Free Speech, and the Muslim Community in the United Kingdom Versus the United States*, 21 EMORY INT'L L. REV. 711, 744 (2007).

86. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 516–17 (2012) ("[E]ach of these surveillance efforts began as a limited inquiry but 'gradually extended to capture more information from a broader range of individuals and organizations.'").

their communications, publications, internet searches, and who they talk to because of surveillance."[87] Political speech is at the very heart of the First Amendment,[88] yet speech, particularly pertaining to political ideas, is chilled or censured due to (over-)surveillance by the government.

1. China's Cybersecurity Measures

In light of the growing governmental surveillance in many democracies, it is helpful to look to the cybersecurity measures in China and the country's results in cybersecurity and surveillance. China has adopted a different approach to protect its country from cyberattacks than most democracies by dramatically increasing surveillance and preventing the use of many social media sites such as Facebook, Twitter, and Google.[89] The government blocks certain web searches, monitors email accounts for anti-government opinions, and compels the country's tech firms to remove certain contents from their servers.[90] China has also historically slowed down many sites, including Google, with its filtering technology, forcing its citizens to use other quicker sites that are easily monitored by the Chinese government.[91]

Over the past few years, China has increased its cybersecurity laws and surveillance measures.[92] These new laws strengthen the government's control over the internet and generally restrict foreign companies from publishing online content.[93] Chinese authorities have also targeted virtual private networks ("VPNs") to prevent circumvention of the country's internet laws, and the country may also require people to

87. Brynne O'Neal, *What Americans Actually Do When the Government Is Watching*, BRENNAN CTR. FOR JUST. (July 20, 2015), https://www.brennancenter.org/blog/what-americans-actually-do-when-government-watching.

88. Lane v. Franks, 134 S. Ct. 2369, 2377 (2014) ("Speech by citizens on matters of public concern lies at the heart of the First Amendment, which 'was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'").

89. Greg Wilford, *China Launches Internet Crackdown to Make It Harder for People to Avoid Its 'Great Firewall'*, INDEP. (Aug. 6, 2017, 3:43 PM), http://www.independent.co.uk/news/world/asia/china-internet-crackdown-virtual-private-networks-vpns-facebook-twitter-youtube-google-whatsapp-a7879641.html.

90. *China's Top Cyber Watchdog Is Making More Demands on Tech Firms*, REUTERS (July 20, 2017), http://fortune.com/2017/07/20/chinese-censorship-tencent-baidu/.

91. Jyh-An Lee et al., *Searching for Internet Freedom in China: A Case Study on Google's China Experience*, 31 CARDOZO ARTS & ENT. L.J. 405, 413 (2013).

92. Keith Bradsher, *China Blocks WhatsApp, Broadening Online Censorship*, N.Y. TIMES (Sept. 25, 2017), https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html.

93. Simon Denyer, *China's Scary Lesson to the World: Censoring the Internet Works*, WASH. POST (May 23, 2016), https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.881f5fdc8e7a.

register for online forums using their real names.[94] Though internet companies in China were already required to censor speech and to assist the government to track individuals who are critical of the government, many are concerned the new laws passed in the past few years will further stifle speech online and control expression.[95] With the new laws, many foreign companies are concerned that they will be forced to hand over intellectual property and to store personal information and important business data in China to aid the government in monitoring its citizens.[96] Furthermore, these strict cybersecurity laws are generally believed to restrict international business and hamper technological competitiveness.[97]

China suppresses significant amounts of speech within the country in an effort to control expression, both on and off the internet. When coupled with the very real threat of surveillance, detention, and imprisonment, this censorship and government surveillance prevents speech on many subjects, including those that relate to human rights issues.[98] This "Great Firewall of China" forces people to over-censor their own speech because the country's internet laws are ambiguous and people and corporations cannot predict the government's application of those laws.[99]

Yet at a time when many democracies face the problems of cyberattacks, similar issues have not appeared as prominently in China.[100] Other countries have similarly followed China's lead, as seen by the banning of Facebook and Twitter prior to elections in Indonesia and some African countries.[101] This preference for content control can more

94. Cheang Ming & Saheli Roy Choudhury, *China Has Launched Another Crackdown on the Internet—but It's Different This Time*, CNBC (Oct. 26, 2017, 1:14 AM) https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html.

95. *China: Proposed Cybersecurity Law Will Bolster Censorship*, HUM. RTS. WATCH (Aug. 4, 2015, 5:50 PM), https://www.hrw.org/news/2015/08/04/china-proposed-cybersecurity-law-will-bolster-censorship.

96. *China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears*, GUARDIAN (Nov. 7, 2016, 1:33 PM), https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears.

97. *China's Cyber Security Law and Its Chilling Effects*, FIN. TIMES (June 1, 2017), https://www.ft.com/content/60913b9e-46b9-11e7-8519-9f94ee97d996.

98. Roseann Rife, *Opinion: The Chilling Reality of China's Cyberwar on Free Speech*, CNN (Mar. 25, 2015, 4:48 AM), http://www.cnn.com/2015/03/24/opinions/china-internet-dissent-roseann-rife/index.html.

99. Yutian Ling, *Upholding Free Speech and Privacy Online: A Legal-Based and Market-Based Approach for Internet Companies in China*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 175, 180–86 (2011).

100. Steven Lee Myers & Sui-Lee Wee, *As U.S. Confronts Internet's Disruptions, China Feels Vindicated*, N.Y. TIMES (Oct. 16, 2017), https://www.nytimes.com/2017/10/16/world/asia/china-internet-cyber-control.html.

101. Paul Mozur & Mark Scott, *Leverage for Globe's Gullible: Facebook's Fake News Problem*, N.Y. TIMES, Nov. 18, 2016, at A1.

properly be termed "information security," but information security is really so interconnected with cybersecurity that these methods can reasonably be viewed as pursuing one objective.[102] But even with the strictest government surveillance and censorship, technology advances too fast and countries, including China, have not kept out disinformation.[103]

C. DISINFORMATION AFFECTS INFORMED VOTING IN DEMOCRACIES

The second vital pillar of democracy discussed in this Article is informed voting. Democracy requires informed voters;[104] informed voters require truthful information, and voters can only trust the information if they trust the source. This past year showed the world just how much the internet and media can affect democratic elections. With the pervasive disinformation efforts in the U.S. presidential election, the French election, the German election, and the Catalonian election, countries are increasing their cybersecurity protections and working towards methods aimed at preventing false stories from interfering in the basic tenets of their democracies.[105] Because of the prevalence of disinformation, trust in the media has declined significantly, particularly as the role of social media increases.[106]

Many countries, including Russia, France, Israel, India, Japan, and Taiwan, also engage in cyber-espionage.[107] The United States is included in this group and conducts extensive "cyberspying."[108] In addition to its "shield" in cybersecurity described above, China engages in cyberattacks and cyber-espionage as well.[109] Due to modern advances in technology, the almost instantaneous rate of information dissemination through the internet and social media has made cyber-espionage much easier. For

102. Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 157–58 (2014).

103. *Fake News Isn't Just for U.S. as China Gets Billions of Claims*, BLOOMBERG NEWS (Oct. 10, 2017, 1:44 AM), https://www.bloomberg.com/news/articles/2017-10-10/china-s-google-checks-3-billion-fake-news-claims-every-year.

104. Stanley Ingber, *The Marketplace of Ideas: A Legitimizing Myth*, 1984 DUKE L.J. 1, 3–4 (1984) ("In order for a democracy to function effectively, the citizens whose decisions control its operation must be intelligent and informed.").

105. *See* Morgan Chalfant, *Denmark, Sweden Team Up to Counter Russian 'Fake News*,*'* THE HILL (Aug. 31, 2017, 11:03 AM), http://thehill.com/policy/cybersecurity/348693-denmark-sweden-team-up-to-counter-russian-fake-news.

106. Mathew Ingram, *Here's Why Trust in the Media Is at an All-Time Low*, FORTUNE (Sept. 15, 2016), http://fortune.com/2016/09/15/trust-in-media/.

107. Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 259 (2013).

108. Jacob Davidson, *China Accuses U.S. of Hypocrisy on Cyberattacks*, TIME (July 1, 2013), http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

109. Teplinsky, *supra* note 107, at 259.

example, Russian bots spread false information through Twitter and Facebook, creating fake accounts used to sow distrust in political news relating to the U.S. election.[110]

Democracy requires political participation, particularly informed voting.[111] The democratic principle of informed voting does not require that every citizen understand every issue; rather democracies need a general, well-informed citizenry who are active in the political process.[112] Disinformation and false reports prevent voters from getting the information necessary to make an informed decision on elected representatives and laws.[113] False information also prevents voters from trusting reliable sources and creates doubt in news that may actually be true.[114] By leaking partial or completely false information or even true, yet confidential, information, individuals or foreign governments can shape public opinion and interfere with democratic voting. Both democracy and information warfare have been around for centuries, but this spread of false information and the ease at which it can be done causes many to fear the destruction of our democratic values.[115]

IV. PROTECTING DEMOCRACY FROM CYBERSECURITY AND THE INTERNET

Democracy is a learning process,[116] and in the history of democracies, the internet is just now emerging as a change in our society. Most technological innovations in communication have presented the same problems throughout history, to varying degrees.[117] With regards to the internet and cybersecurity, we have not had time to adjust and learn from our mistakes. This form of government has gone through centuries of instability and uncertainty, yet it is still here and democracy is more

110. Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

111. Tabatha Abu El-Haj, *Friends, Associates, and Associations: Theoretically and Empirically Grounding the Freedom of Association*, 56 ARIZ. L. REV. 53, 96 (2014).

112. DAHL, *supra* note 13, at 339 (asserting that democracy "does not require that every citizen should be informed and active on every major issue . . . What is required instead is a critical mass of well-informed citizens large enough and active enough to anchor the process."); R. Randall Rainey, S.J. & William Rehg, S.J., *The Marketplace of Ideas, the Public Interest, and Federal Regulation of the Electronic Media: Implications of Habermas' Theory of Democracy*, 69 S. CAL. L. REV. 1923, 1970 n.117 (1996).

113. Amy Lee Rosen, *Shareholders Demand Google and Facebook Report on Fake News Policies*, CQ ROLL CALL, 2017 WL 460653 ("The 'fake news' controversy undermines a core tenet of U.S. democracy—an informed electorate.").

114. Sabrina Tavernise, *As Fake News Spreads Lies, More Readers Shrug at the Truth*, N.Y. TIMES (Dec. 6, 2016), https://www.nytimes.com/2016/12/06/us/fake-news-partisan-republican-democrat.html.

115. Janine Young Kim, *On Race and Persuasion*, 20 CUNY L. REV. 505, 506 n.12 (2017).

116. JUDITH M. GREEN, DEEP DEMOCRACY: COMMUNITY, DIVERSITY, AND TRANSFORMATION viii (1999).

117. Anupam Chander, *Whose Republic?*, 69 U. CHI. L. REV. 1479, 1499 (2002).

widespread than any other time in history.[118] Democracy has prevailed against all odds, and the struggle will continue as democratic values spread.[119] The events in this past election, particularly the increase in the use of social media in our political processes and campaigns, is another evolution in the history of democracy. Among its many other benefits, the internet allows people who otherwise would have no voice to express their political views, and those with no ability to physically "assemble" and organize as the First Amendment freely protects.[120] Those who were previously disenfranchised or effectively silenced now have an accessible method to spread political ideas without needing the support of the traditional media.[121]

The internet has allowed those problems discussed in the Parts above, yet it also provides better opportunities to promote and protect our democracy: the ability to spread political information to voters quickly and effectively allows people to speak freely throughout the world. How we respond to these new challenges will define the next age of democracy. To be sure, Professor Persily is correct that the "prevalence of false stories online erects barriers to educated political decision making . . ."[122] and that democracy's greatest benefits can be its biggest downfalls.[123] As recent events have shown, demagogues can use this new technology to appeal to the debasing impulses of people all over the world.[124] But the internet has also provided a voice to people often left out of the political process: look to former Vermont Governor Howard Dean's campaign for the 2004 Democratic nomination[125] and Bernie Sanders' 2016 presidential run. Both of these campaigns assembled hundreds of thousands of people from across the country and raised money and assistance from individuals who previously could not

118. *What's Gone Wrong with Democracy*, ECONOMIST, Mar. 1, 2014, at 47, 48.

119. Imran Khan, *The Fight for Democracy Goes On*, GUARDIAN (Apr. 15, 2009, 5:00 AM), https://www.theguardian.com/commentisfree/libertycentral/2009/apr/14/democracy-revolution-freedom.

120. *Transcript: Free to State: A New Era for the First Amendment*, WASH. POST (June 21, 2017), https://www.washingtonpost.com/blogs/post-live/wp/2017/06/21/transcript-free-to-state-a-new-era-for-the-first-amendment/?utm_term=.d8fd06c655f2.

121. Chander, *supra* note 117, at 1498.

122. Persily, *supra* note 7, at 68.

123. Persily, *supra* note 7, at 71; *see also* Justin McHugh, *Review of: I Know Who You Are and I Saw What You Did (Social Networks and the Death of Privacy)*, 31 SYRACUSE J. SCI. & TECH. L. 132, 141 (2015) ("It is ironic how social media sites are helping to promote democracy at the same time as they are taking away our freedoms.").

124. McHugh, *supra* note 123, at 141.

125. Anthony E. Varona, *Changing Channels and Bridging Divides: The Failure and Redemption of American Broadcast Television Regulation*, 6 MINN. J.L. SCI. & TECH. 1, 101 (2004).

organize behind a unified message.[126] We can look to the influence that social media has on public policy and politics, such as the spreading of political statements or ideas through videos and online messaging[127] and the unprecedented ability to petition the government.[128] The internet provides enhanced communication and gives citizens a chance to be more politically involved and knowledgeable. The internet can provide for more government transparency, allow voters to become more informed, and lead to better democratic governance.[129] The internet can even promote the free flow of ideas, sparking debate and engagement to the entire world rather than simply those in charge.

The recent foreign interference in a democratic election is troubling. But this does not mean that democracy will fail. Most of 20th century international relations were characterized as a battle between democracy and opposing forces, such as fascism or communism.[130] The spread of disinformation can impair democracy, but democracies will respond and adapt. *How* democracy will respond is the next step. The internet and cybersecurity can enhance democracy if used effectively.[131] Our efforts must be to ensure the internet and cybersecurity—the necessary response to cyberattacks brought by technological innovation—are put to socially beneficial uses that promote and strengthen democracy.[132] The internet is and will continue to be essential to democracy,[133] and we must ensure that cybersecurity protects democracies by promoting democratic values. When considering the best measure of response, we must remember not to impact our fundamental pillars of democracy, particularly free speech and informed voting. To maintain the best version of free speech ideals, we cannot censor what citizens say based

126. Peter Overby, *Will The Millions Of People Who Gave Money to Bernie Sanders Give to Democrats?*, NPR (June 15, 2016, 4:28 PM), https://www.npr.org/2016/06/15/482206235/will-future-candidates-be-able-to-raise-money-the-sanders-way.

127. Kevin Gregg, *"Text 'Revolution' to Vote": Social Media's Effect on Popular Consent and Legitimacy of New Regimes*, 31 B.U. INT'L L.J. 315, 328 (2013).

128. Ross Rinehart, *"Friending" and "Following" the Government: How the Public Forum and Government Speech Doctrines Discourage the Government's Social Media Presence*, 22 S. CAL. INTERDISC. L.J. 781, 785 (2013).

129. *See generally* Grichawat Lowatcharin & Charles E. Menifield, *Determinants of Internet-enabled Transparency at the Local Level: A Study of Midwestern County Web Sites*, 47 STATE & LOCAL GOV'T REV. 102 (2015) (asserting that government transparency through the internet "provides citizens with far greater potential to observe and understand what is going on in government, blurs the boundaries between citizens and state, and opens up the processes for greater scrutiny").

130. SHERI BERMAN, THE PRIMACY OF POLITICS: SOCIAL DEMOCRACY AND THE MAKING OF EUROPE'S TWENTIETH CENTURY 1 (2006).

131. Neil Weinstock Netanel, *Cyberspace 2.0*, 79 TEX. L. REV. 447, 458 (2000).

132. Chander, *supra* note 117, at 1499.

133. Teresa Scassa & Robert J. Currie, *New First Principles? Assessing the Internet's Challenges to Jurisdiction*, 42 GEO. J. INT'L L. 1017, 1044 (2011).

solely on its content. Similarly, completely banning certain types of speech on the internet creates the same problems for democracy. Censorship of speech is generally the antithesis to the foundation of democracy, and while the U.S. protection of speech is broader than most nations, if not all,[134] democracies need to be wary of censoring speech on the internet.

There has been significant discussion on how to respond to the increase of false information. One such response is to hold internet and social media platforms responsible for their algorithms when false information is pushed due to monetization of publicity.[135] This response argues that internet algorithms—such as the ones Google uses when individuals search for key words—need to balance all interests of a democracy, including accountability.[136] Companies such as Facebook, Google, and Twitter do not actually create these false stories or reports, but they do allow disinformation to spread when they push news in response to a search or facilitate peer-to-peer sharing. Another suggested response to the spread of false stories or information is to require social media platforms to file all political advertising and political bots with election officials to make it clear to users who is paying for or disseminating the advertising,[137] including issue ads.[138] Private social media platforms can also use their terms and conditions, which users agree to by using the site, and upon which their use is conditioned, to reduce spam sites and allow their users to flag false articles.[139] Some countries even fine social media platforms for failing to remove illegal content after being notified of its existence.[140]

In the democratic context, the truth is the best protection against disinformation. As Justice Brandeis so eloquently put: "If there be a time to expose through discussion the falsehood and fallacies, to avert the evil

134. Gray, *supra* note 84.

135. Adam Segal, *Protecting Democracy from Online Disinformation Requires Better Algorithms, Not Censorship*, COUNCIL ON FOREIGN REL. (Aug. 21, 2017), https://www.cfr.org/blog/protecting-democracy-online-disinformation-requires-better-algorithms-not-censorship.

136. *Id.*

137. Kelcee Griffis, *Watchdog Orgs. Urge Transparency in Online Election Ads*, LAW360 (Nov. 13, 2017, 8:55 PM), https://www.law360.com/cybersecurity-privacy/articles/984340/watchdog-orgs-urge-transparency-in-online-election-ads; Philip Howard & Bence Kollanyi, *Social Media Companies Must Respond to the Sinister Reality Behind Fake News*, GUARDIAN (Sept. 30, 2017, 7:03 PM), https://www.theguardian.com/media/2017/sep/30/social-media-companies-fake-news-us-election.

138. Karen Kornbluh, *Bringing Transparency and Accountability to Online Political Ads*, COUNCIL ON FOREIGN REL. (Oct. 30, 2017), https://www.cfr.org/blog/bringing-transparency-and-accountability-online-political-ads.

139. Richard Gray, *Lies, Propaganda, and Fake News: A Challenge for Our Age*, BBC: FUTURE NOW (Mar. 1, 2017), http://www.bbc.com/future/story/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age.

140. Anya Schiffrin, *How Europe Fights Fake News*, COLUM. JOURNALISM REV. (Oct. 26, 2017), https://www.cjr.org/watchdog/europe-fights-fake-news-facebook-twitter-google.php.

by the process of education the remedy to be applied is more speech, not enforced silence."[141] It is one of the reasons why courts use the adversarial system: to effectively determine the truth.[142] The electorate, including the news media, must ensure that truthful information is used to counter any falsehoods that are spread. This is why democracy requires active participation by its citizens.

However, for democracy to survive, democratic states must gather and disseminate accurate facts and information to their citizenry at a faster pace than states currently do.[143] First, and most importantly, is the acknowledgement of the problem of foreign interference and influence in democracies through general awareness and transparency. Additionally, social media platforms must police their internet platforms for false information and dangerous content intended to undermine democracies.[144] Private companies like Facebook and Google have already begun this response, and independent citizenry groups have attempted to create fact-checking processes to combat disinformation.[145] Lobbying groups continue to push for more transparency in the internet and social media platforms on how news is spread. Governmental responses need to include this transparency as well, such as by keeping voters informed of the state's action. Another effort to combat false information must be to focus on the algorithms used by sites and social media.[146] Efforts to respond to false information have grown, even if difficulties with those responses continue to arise.[147] One suggested effort to improve fact-checking processes has been to create a bot which follows specific news searches and targets specific users spreading false information to provide context or corrections when that false information is spread.[148] Journalists, fact-checkers, and social media platforms can also partner to effectively and quickly counter viral false information.

---

141. Whitney v. Cal., 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

142. Monroe H. Freedman, *Our Constitutionalized Adversary System*, 1 CHAP. L. REV. 57, 73 (1998).

143. John O. McGinnis, *Laws for Learning in an Age of Acceleration*, 53 WM. & MARY L. REV. 305, 308 (2011).

144. Keir Giles, *Countering Russian Information Operations in the Age of Social Media*, COUNCIL ON FOREIGN REL. (Nov. 21, 2017), https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

145. Nick Wingfield et al., *Google and Facebook Take Aim at Fake News Sites*, N.Y. TIMES (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html.

146. Segal, *supra* note 135.

147. Gray, *supra* note 139.

148. Andrea Stroppa & Michael Hanley, *How Can We Defeat Fake News?*, WORLD ECON. F. (Feb. 8, 2017), https://www.weforum.org/agenda/2017/02/how-can-we-defeat-fake-news-automate-the-right-to-reply.

These responses have not been realized fast enough, but steps toward countering disinformation with the truth while protecting the freedom of speech will not happen overnight. After this election and the recent attacks on democratic elections throughout the year, the efforts to counter disinformation are increasing and effective measures to countering these attacks on our democracy should begin to emerge: "truth will out."[149] Democracies will learn to adapt and protect themselves against false information and cyberattacks, and this learning process will continue throughout the cyber age.

CONCLUSION

Democracy will only be destroyed by the internet if we allow it to undermine democratic values. "To renew our country, we only need to remember our values . . . The health of the democratic spirit itself is at issue."[150] Democracy will be strong as long as we remember and adhere to our democratic values, particularly protecting free speech and promoting informed voting. Throughout history, nations change their political and governmental structure, pushed primarily by changing technology and evolving warfare. Democracy changes as well. As long as the nation retains underlying democratic values, democracy will thrive. Whether likened to Isaac Newton's Laws of Physics—every action has an equal and opposite reaction—or Justice Ginsberg's Pendulum,[151] democracy will react and respond to the challenges rising from the internet and adjust to those threats accordingly.

This past year has raised many questions regarding democracy throughout the world, particularly relating to free speech and informed voting. Outside interference in democratic elections through cyber communication and expansive government surveillance do threaten democratic values. Professor Nathaniel Persily and I look to the same events in this past presidential election, and while some see an ongoing "deterioration in democratic values,"[152] I see an opportunity to strengthen our democracy for the future. Maybe the difference here is just faith in the resiliency of democracy itself and the ability of democracy to change. Technology got us into this mess, but it will save us if that

149. WILLIAM SHAKESPEARE, MERCHANT OF VENICE act 2, sc. 2.

150. Domenico Montanaro, *George W. Bush Slams 'Bigotry,' Politics of Populism That Led to Trump, Sanders*, NPR (Oct. 19, 2017, 1:23 PM), http://www.npr.org/2017/10/19/558788556/george-w-bush-slams-bigotry-politics-of-populism-that-led-to-trump-sanders.

151. Kristine Phillips, *Ruth Bader Ginsburg on Trump's Presidency: 'We Are Not Experiencing the Best of Times,'* WASH. POST: THE FIX (Feb. 27, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/02/24/ruth-bader-ginsburg-on-trumps-presidency-we-are-not-experiencing-the-best-of-times/?utm_term=.9392ac969b8b.

152. Persily, *supra* note 7, at 74.

technology is used and regulated correctly. How we use technology will prevent the breakdown of democratic values, and democracy will find a way to adapt to challenges of the cyber age.