BEYOND FIGHTING WORDS: RECONCEPTUALIZING INFORMATION WARFARE AND ITS LEGAL BARRIERS

Laura B. West*

Despite exhausting levels of discourse surrounding information warfare and the dramatic rise of these operations in the information environment, the United States still lacks a unified understanding and approach to countering these threats. The U.S. government continues to advocate for the notion that combating information warfare requires a whole-of-society approach. The problem with this approach is that those aspects of society primarily engaged in the fight—government agencies, private companies, media, academia, and individuals—all define and understand information warfare differently.

Government's failure to adopt a common core definition of information warfare to shape the U.S. national consciousness presents its own threat to national security because it leads to an incomplete understanding of all its avenues of attack. Society is left to believe that information warfare is merely about the words spoken—the "new fighting words." U.S. laws and policies that restrict regulating those words or speech may then lead many to believe that the United States has its hands tied when it comes to combating information warfare and its associated harms. But this is an incomplete picture of the problem and its solutions.

In its most simplistic form, information warfare is about gaining access to people. Once the United States accepts this more

* Major Laura West is a Judge Advocate in the U.S. Army and currently serves as the Deputy Chief of National Security Law at U.S. Cyber Command. The views expressed in this article are those of the author and do not necessarily represent the views of the Department of Defense or any other government agency. The author wants to thank Professors Julie Cohen and Todd Huntley for their expert instruction and advice that helped shape this article.

simplistic and holistic definition of information warfare, and reconceives of related information harms, content is exposed as only one main avenue of attack—and not an indefensible one at that. In addition to content or speech, data practices and norm building are utilized to maliciously gain access to people in the United States for political ends. Data and norms, therefore, are two additional avenues of attack for information warfare that require the U.S. government's attention. Laws and policies within all three of these major areas of attack need to be reexamined to facilitate the fight against information warfare and overcome some assumed domestic legal barriers.

The goal of this article is essentially twofold: to arrive at a common U.S. national definition of information warfare by reframing its surrounding discourse, and to introduce new ways of thinking or additional insights about how U.S. domestic law works toward combating information warfare as it has been shaped in today's information environment. In some instances, our domestic laws currently do offer avenues for combating information warfare. In other instances, our laws might need to be reconceptualized in order to do so. In the end, this article is meant to provoke those conversations required for the United States to regain its stance as a leader nation in the fight against information warfare and champion for democracy, all while better understanding the information harms of today and into the future.

I. INTRODUCTION: KNOW YOURSELF, AMERICA

"If you know the enemy and know yourself, you need not fear the result of a hundred battles." Sun Tzu, The Art of War[1]

One of the most quoted phrases in commentary on warfare is from Sun Tzu, the ancient Chinese philosopher of war, who stated "know the enemy."[2] The appearance of this quote is so expected, its use verging on cliché, that its absence would seem almost an aberration to students of warfare. As society continues to label information harms as "information warfare"—the prevailing terminology today—Sun Tzu's quote accordingly makes its appearance here. In fact, this article is framed around this quote; though, the focus is on the part that is often omitted: "know yourself."[3] This article addresses ways the United States can better know itself in the context of information warfare through a U.S. domestic legal lens.[4] While the United States' outward-looking approach to combating information harms abroad has meaningful effects, successfully addressing the information warfare fight requires an increased focus on the homeland, with a close examination and reconceptualization of U.S. domestic laws and policies.

Scholars argue that U.S. laws hamper the fight against information warfare.[5] Although practically true in a sense, such conclusions are framed by only a partial picture of the domestic legal landscape. Fighting information warfare is not only about content and

---

[1] SUN TZU, THE ART OF WAR 24-25 (Lionel Giles ed., trans. 1910).
[2] *Id.* at 24.
[3] *Id.*
[4] In 1999, the Department of Defense published a legal assessment of information operations with a focus on the international law aspect of these operations. Since then, there has not been any significant government publication reassessing the legal issues surrounding information operations, especially from a domestic law standpoint. *See* U.S. Dep't of Def. Off. of Gen. Couns., An Assessment of International Legal Issues in Information Operations (1991).
[5] *See* Jill I. Goldenziel & Manal Cheema, *The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare*, 22 J. CONST. L. 81, 85 (2019) ("[T]he United States' own laws tie its hands in its fight against information warfare.").

the First Amendment—the United States must look beyond those fighting words; albeit, these aspects carry significant influence. One way to think of the information environment in a militaristic sense is that content is the main effort or main avenue of attack, flanked by supporting efforts of data practices and norms. Relatedly, information warfare is also influenced by emerging technology as well as U.S. perspectives and policies on innovation, strategic competition, and democratic ideals. All of these policy factors drive U.S. domestic law to where it is today for addressing information warfare. Understanding these major influencing policies and avenues of attack, therefore, is imperative to understanding the overall domestic legal landscape applicable to information warfare and how the law can be operationalized to respond to such threats. This article intends to address these main avenues of attack spanning the information environment—content, data, and norms—while weaving in a discussion of influencing policies.

Focusing on "knowing yourself," however, does not mean the United States can ignore the other half of the equation; Sun Tzu advised that winning battles requires both knowing the enemy and yourself. Before the U.S. government and society can even begin to understand those major attack vectors and policy factors facilitating information warfare in the United States, there must be a clear understanding of the threats or the "enemy" that is information warfare. This alone is a daunting task. Nevertheless, if the U.S. government continues to advocate for the notion that combating information warfare is a whole-of-society endeavor,[6] then there must be a common and clear understanding by society of what it constitutes and ultimately aims to regulate as a harmful activity. The problem with this approach is that those aspects of society primarily engaged in the fight—government agencies, private companies, media, academia, and individuals—all define and understand information warfare differently, looking only at their specific mission or area of focus. A 2018 Congressional Research Report highlighted this problem as an

[6] CATHERINE A. THEOHARY, CONG. RSCH SERV., R45142, INFORMATION WARFARE: ISSUES FOR CONGRESS 1(2018).

issue for Congress to address in the future.[7] To date, there is still no common core definition to shape the U.S. national consciousness.[8] The government's failure to define and establish a unified concept of information warfare presents its own threat to national security because it leads to an incomplete understanding of all its avenues of attack within the United States and the harms that lead to the activity requiring regulation.

To define information warfare to study it from a domestic legal perspective, and better understand it as a whole-of-society endeavor, this article intends to arrive at a common core understanding for decision-makers of all types, including those of law, policy, war, the market, and speech. A definition of this sort needs to discard ambiguity, appreciate the full consequences of information harms, and transcend boundaries between government, the private sector, and individuals.[9] It also needs to send an international message for how the United States views information warfare, and more specifically, how the United States views information harms or information violence, both presently and into the future.

To fill this gap, this article offers the general definition of information warfare as maliciously accessing people in the information environment, intending to manipulate or disrupt, for

[7] *Id.* at 6.

[8] *See, e.g.*, Conrad Crane, *The United States Needs an Information Warfare Command: A Historical Examination*, War On The Rocks (June 14, 2019), https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/ ("For decades, the United States has engaged in information operations but lacked a unified understanding of the concept that is sorely needed to respond effectively to today's adversaries.").

[9] Scholars suggested abandoning the terms information operations or information warfare altogether because they are so "beset by ambiguity" as defined, covering a wide array of operations from planning to execution, and fail to capture the public's and private sector's general conception of the term. *See* Christopher Paul, *Is It Time to Abandon the Term Information Operations?*, RAND CORP. (Mar. 13, 2019), https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html.

political ends. At its core, though, it is simply access to people.[10] Fighting, waging, or stopping information warfare requires an understanding of how to control or protect that access. Upon the initial revelation of the pure simplicity of this proposition, a solution for the American people to combat information warfare through the law seemed to take on quite the opposite character—one that was unreachable, untenable, or utterly complex. Many scholars have already made this exact point by stating the obvious, the United States is not China.[11] The United States does not wall off the nation with immense firewalls and implement grand-scale government interference and overwatch of its people.[12]

On the contrary, the United States strives to be an open and free nation.[13] Americans believe in the freedom of speech, information, and ideas. Rooted in these beliefs is the notion that Americans value all ideas—good or bad. Ideas are meant to have free entry into the speech marketplace, a notional market that will allow for the truth to work itself out amongst the noise, and help Americans individually realize their autonomy and informational self-determination. Americans also believe in a free internet, which is considered a cornerstone to achieving innovation, democracy, and dominance in today's strategic competition.[14] With these beliefs comes the fact that Americans are assumed to value a light-touch regulatory scheme over the internet, one free of government interference and

[10] Professor Laura Donohue offered this more simplistic explanation or core definition during a brainstorming session for this article in February 2020.
[11] JIM SCIUTTO, THE SHADOW WAR: INSIDE RUSSIA'S AND CHINA'S SECRET OPERATIONS TO DEFEAT AMERICA 259 (2019).
[12] *See* Eric Rosenback & Katherine Manstead, *Can Democracy Survive in the Information Age?*, Belfer Ctr. for Sci. and Int'l Affs., Harv. Kennedy Sch. 3, 11 (Oct. 2018) ("China is willing to use offensive measures to suppress information that challenges its domestic control of information.").
[13] *See* Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How A Digital World Disadvantages the United States in its International Relations*, Aegis Series Paper No. 1806, 1 (2018).
[14] *Cf.* Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMEND INST. (June 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom.

intrusion.[15] Needless to say, when balancing all these ideals, solutions to the information warfare problem under the U.S. legal and value system are indeed easier said than done.

Therefore, a conclusion that U.S. laws hamper the fight against information warfare is a logical one. Yet, this article intends to show that the task, while logically difficult and requiring a multifaceted legal and policy approach, is not an impossible one. Reconceptualizing or reframing our laws and policies and how we approach reform in certain areas, all while maintaining and pursuing the full realization of our ideals, can make the United States a leader in combating information warfare.

To set out on this journey to redefine information warfare and reconceptualize those domestic laws that potentially hamper the fight against it, a roadmap is required. The three main avenues for attack in conducting information warfare—content, data, and norms—are selected to serve as this rough roadmap because of their fundamental ability to control access to people. These main areas will be addressed in the sections of this article below, following a reframing of our understanding of information warfare in an attempt to arrive at a common definition in Part II. The focus of the U.S. domestic legal taxonomy is discussed in Parts III and IV, which analyze the main ways in which access is gained to people through content and data respectively. These parts of the article introduce the basic controlling legal frameworks and how the law can be understood or reframed to be more effective in combating information warfare. To round out this domestic law survey, Part V serves as a brief introduction to how norms affect our domestic legal landscape on the fringes and play a critical role in achieving any significant reform at home.

[15] *See* Fed. Comm. Commission, *In the Matter of Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order*, WC Docket No. 17-108, 7-8 (Jan. 4, 2018).

The goal of this article is twofold: to arrive at a common definition by reframing the discourse surrounding information warfare, and to introduce new ways of thinking or additional insights about how U.S. domestic law interacts with and can work toward combating this way of warfare as it has been shaped in today's information environment. This article shows that in some instances, our domestic laws currently offer avenues for combating information warfare. Paradoxically, this comes in the form of rethinking about the First Amendment and its underlying ideals by understanding that it is not absolute and does not foreclose regulation of malicious activity to protect against information harms. In other instances, however, U.S. laws must be reconceptualized or dramatically reformed to fend off information warfare. While the First Amendment and addressing harmful content may not pose as much of a bar to regulation as assumed when you start looking closer at the activity, it is data practices and the individual privacy landscape that requires considerable attention and reform efforts from lawmakers and policymakers.

In the end, this article is meant to provoke some of those conversations required for the United States to become a leading nation in the fight against information warfare and reestablish itself as a champion for democracy.[16] Studying these areas of the law is merely the first step for the United States to know itself as a nation in combating information warfare.

II. REFRAMING OUR UNDERSTANDING OF INFORMATION WARFARE

Information warfare has taken on many identities, increasingly so within the past few years. Government organizations,[17]

[16] *Cf.* Goldsmith, *supra* note 14, at 8 (arguing that the notion of internet freedom has caused damage to our democracy at home).

[17] The U.S. Department of Justice refers to what might constitute information warfare as "malign foreign influence operations" that "include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public

non-government organizations,[18] news media,[19] academia,[20] businesses,[21] and the public[22] attached different meanings to the term over the years. For this reason, the concept of information warfare generally evaded a standardized and established definition to inform our national consciousness and guide reasoned debate.[23]

---

discourse to achieve strategic geopolitical objectives." U.S. Dep't of Just., Rep. of the Att'y Gen's Cyber Digital Task Force 1-2 (2018). In contrast, the Department of Defense refers generally to "information operations" that constitute a wide range of "information-related capabilities" that work "to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." Army Techniques Publication, No. 3-13.1, The Conduct of Information Operations 1-1 (2018). *See also* Joint Publication, 3-13, Information Operations ix (2012).

[18] *See*, ROGER C. MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR (1996); David Stupples, *What is Information Warfare?*, WORLD ECON. F. (Dec. 3, 2015), https://www.weforum.org/agenda/2015/12/what-is-information-warfare/.

[19] *See* Ina Fried, *Coronavirus Misinformation is a Tricky Foe for Tech*, AXOIS (May 11, 2020), https://www.axios.com/coronavirus-misinformation-foe-tech-a5b347e9-99d6-4d4c-9232-02e405253427.html.

[20] *See* Goldenziel and Cheema, *supra* note 5, at 83-84; *cf.* SIVA VAIDHYANATHAN, ANTI-SOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 11 (2018) (defining fake news, propaganda, garbage or disinformation as the same: "a constant and alarming undermining of public trust in expertise and the possibility of rational deliberation and debate").

[21] *See* Jen Weedon et al., Information Operations and Facebook, Facebook, 4 (Apr. 27, 2017), https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf#page=4 (defining information operations as "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome"). A RAND study asserts that Facebook's definition "promotes an understanding of information operations that is inconsistent with both the colloquial and the formal Department of Defense usage—and one that is quite pejorative. *See* Paul, supra note 9.

[22] *See id.* ("The general public's understanding of information operations is much closer to the Facebook definition than to the Department of Defense definition—yet another reason for the department to move away from the term.")

[23] *Compare* L. Scott Johnson, Toward a Functional Model of Information Warfare: A Major Intelligence Challenge, CIA (last accessed May 12, 2020), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html, *with* THEOHARY, *supra* note 6, at 6, *and* Crane, *supra* note 8.

The flurry of differing definitions and understanding of the term exponentially increased throughout public discourse due to the 2016 U.S. election interference by Russia, which has become the United States' poster child for information warfare.[24] The debate around information warfare surged in recent years as a result, focused mainly on the role it played in political campaigns.[25] Such intense focus on one specific type of information warfare, however, hampers our collective ability to achieve a fully-informed understanding of the term. Nevertheless, the focus on the Russian interference in our political system served a vital function of heightening Americans' awareness of the fact that the United States is currently engaged in information warfare. Accordingly, now is the time to address the substantive issues.[26]

Before there can be reasoned debate and cooperation to flesh out these issues between all entities that make up the U.S. national fabric, as well as international partners, the United States needs a collective understanding of information warfare. Society needs to know what they are working together to control or prevent. With this goal in mind, this section outlines the support behind adopting a common general definition of information warfare that is: *maliciously accessing people in the information environment, intending to manipulate or disrupt, for political ends*.

[24] *See* Weedon et al., *supra* note 21.

[25] J. Scott Brennen, *Misinformation: The Evidence On Its Scope, How We Encounter It and Our Perceptions of It*, U. OF OXFORD REUTERS INST. (last accessed May 12, 2020), https://reutersinstitute.politics.ox.ac.uk/risj-review/misinformation-evidence-its-scope-how-we-encounter-it-and-our-perceptions-it.

[26] "If these obstacles, along with others suggested by a historical analysis of the implementation of a new form of warfare, are indeed alive and well today, then there may be a good chance that the substantive issues of information warfare will not be addressed until the United States is actually engaged in an information war." JOINT CONCEPT FOR OPERATING IN THE INFORMATION ENVIRONMENT (JCOIE), JOINT CHIEFS OF STAFF v (2018), (citing Richard Jensen, 1997).

A. Toward a Common Definition: The General Contours of Information Warfare

1. Accessing People

The earliest common use of the term information warfare in the United States dates back to the 1970s when Dr. Tom Rona expanded the field of "cybernetics" beyond just a theory of information.[27] The discipline of "cybernetics," introduced some twenty years prior by Norbert Wiener, focused on the study of communication and control.[28] In Dr. Rona's research, he investigated the competition between competing control systems during the advent of the internet, which he labeled "information warfare."[29]

By the early 1990s, the term information warfare embedded itself as a national security hot topic and catchphrase.[30] Some internal defense agencies even adopted the term for their namesake.[31] During these early developmental years, the 1996 Brown Commission, a congressional commission designed to investigate the roles and capabilities of the United States intelligence community, provided one of the first public statements defining the term.[32] According to the Commission's report, the term information warfare generally meant "activities undertaken by government, groups, or individuals to gain

---

[27] Dan T. Kuehl, Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age, 76 INT'L L. STUD. 35, 36 (2002); *see also* JAMES GLEICK, THE INFORMATION: A HISTORY, A THEORY, A FLOOD 6 (2011).

[28] Kuehl, *supra* note 27, at 36.

[29] *Id.*

[30] Brian C. Lewis, *Information Warfare*, FAS, https://fas.org/irp/eprint/snyder/infowarfare.htm; *see also* Central Intelligence Agency, *The Brown Commission and the Future of Intelligence: A Roundtable Discussion* (last accessed May 12, 2020), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/brown.htm.

[31] FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 73 (2016) (discussing the establishment of the Air Force Information Warfare Center in the early 1990s).

[32] There was an unclassified Defense Department report that defined the term before the Brown commission came out with its public definition. *See* Kuehl, *supra* note 27, at 36.

electronic *access* to information systems in other countries . . . as well as activities undertaken to protect against it."[33]

Around the same time, the Department of Defense (DoD) also published its unclassified definition of information warfare; however, its guidance created the two mutually supporting definitions of "information operations" and "information warfare," a distinction that transcends throughout military doctrine today.[34] Information operations, in its earliest DoD doctrinal conception, was considered those "actions taken to affect adversary information and information systems while defending one's own information and information systems."[35] On the other hand, information warfare was thought of in broader strategic military terms as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[36] These early defense definitions highlighted the Department's thinking that information warfare was to be considered a military activity and only undertaken in a special set of circumstances, those being in times of crisis or conflict.[37] But, as discussed later in this article, these notions

[33] COMMISSION ON THE ROLES AND CAPABILITIES OF THE UNITED STATES INTELLIGENCE COMMUNITY, PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE, *The Role of Intelligence* 26 (1996), https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/context (emphasis added) [hereineafter Brown Comm'n Report].
[34] Kuehl, *supra* note 27, at 36; *cf.* JOINT PUBLICATION 3-13, INFORMATION OPERATIONS xi (2012) (listing the various capabilities that make up the defense conception of information operations); Army Techniques Publication, No. 3-13.1, The Conduct of Information Operations, 1-1 (2018). Today the term information warfare no longer appears in official Department of Defense publications. The term only recently reemerged through Congress surrounding the enactment of the 2020 National Defense Authorization Acts, indicating that the term will likely be reincorporated within defense doctrine in the years to come. *See* National Defense Authorization Act for Fiscal Year 2020, S. Res. 1790, 116th Cong. §§ 1631(g)(3)(C), 5323 (2019) (calling for an assessment of establishing an Army Information Warfare Command and discussing the interdependent relationship with the private sector and defense department to combat foreign information warfare efforts).
[35] Joint Publication 3-13, Information Operations I-9 (1998).
[36] *Id.* at I-11.
[37] Kuehl, *supra* note 27, at 37.

no longer hold up against today's technology or threat environment.[38] Information warfare as we know it today is much broader in scope.

More importantly, the usage of the term information warfare in these early stages did not quite refer to what society might now collectively conceive of as information warfare. Rather, the terminology used then more appropriately referred to what we now view to be cyber warfare or cyberspace operations, borrowing its name from the founding discipline of "cybernetics."[39] In most cases today, we view cyberspace operations as distinct from information operations, taking our cue from the development of military doctrine.[40] Conceptually then, in its simplest form, one can think of cyber warfare or cyberspace operations as accessing networks and systems,[41] whereas information warfare involves accessing people.[42]

[38] Congress recently embraced this understanding of the evolving threat environment as well. *See* H.R. Rep. No. 115-874, 1049-1050 (2018); *see also* 10 U.S.C. § 394 (2019).

[39] *See* The Vocabularist, *How We Use the Word Cyber*, BBC NEWS (Mar. 15, 2016), https://www.bbc.com/news/magazine-35765276.

[40] *Compare* Joint Publication 3-12, Cyberspace Operations (2018), *with* Joint Publication 3-13, Information Operations (2012).

[41] *Cf.* BROWN COMM'N REPORT, *supra* note 33, at 26; Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 821 (2012) (defining a cyber-attack as "any action taken to undermine functions of a computer network for political or national security purpose").

[42] *See* THEOHARY, *supra* note 6, at 1 (arguing that ultimately the target of information warfare activities is human cognition); P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA 18 (2018) (discussing how information warfare tactics are better able to target the spirit of the people). Russia, a nation historically considered "one of the most refined and effective of any in history" described their original information warfare techniques as "active measures" which were meant to influence opinions and/or actions of individuals, governments, and/or publics. George F. Kennan, *'The Inauguration of Organized Political Warfare' [Redacted Version]*, 1 (Apr. 30, 1948), https://digitalarchive.wilsoncenter.org/ document/114320; U.S. DEP'T OF STATE, SOVIET INFLUENCE ACTIVITIES: A REPORT ON ACTIVE MEASURES AND PROPAGANDA, 1986–87, viii (Wash., DC: Bureau of Pub. Aff., 1987). Further, maintaining these two distinct definitions between cyber and information warfare allows the United States to closely mirror how Russia, one of its major adversaries, approaches information warfare. "Russia has divided its information warfare concepts into two parts:

Notwithstanding, this access to people is most often now undertaken through those means of networks and systems and for this reason, the concepts of cyber warfare and information warfare are very much interconnected.[43]

Due to their interconnected nature, some scholars argue for the convergence of both cyber warfare and information warfare to fall under the general title of information warfare.[44] While this might make sense in the limited context of carrying out the military's mission where, in practice, information warfare has increasingly become inseparable from cyberspace operations,[45] there are still important reasons why the terms should remain distinct. First, keeping the terms distinct is critical when trying to arrive at a common core definition to frame our entire national consciousness, not just that of the military.

Second and most importantly, information operations can be far more "contested and controversial" than cyberspace operations.[46] Information operations create opportunities for "significant exposure of the American people and media to U.S. government-created information," which can directly impact fundamental rights.[47] In contrast, cyberspace operations pose far fewer obstacles to individual rights, generally speaking. Such concerns are ever more pressing in

Information technical and information psychological." *Crafting An Information Warfare and Counter-Propaganda Strategy For the Emerging Security Environment: Hearing Before Subcomm. on Emerging Threats and Capabilities of the H. Comm. on Armed Services*, 115th Cong. 7 (2017) (statement of Timothy L. Thomas, Senior Analyst, Foreign Military Studies Office, Fort Leavenworth).

[43] *See* JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS, ix (2018).

[44] *See generally* Martin C. Libicki, *The Convergence of Information Warfare*, 11 STRATEGIC STUD. Q. 49 (2017).

[45] *See* Ellen Nakashima, *U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election,* WASH. POST (Dec. 25, 2019), https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html (citing Professor Robert Chesney).

[46] H.R. Rep. No. 115-874 at 1049.

[47] *Id.*

today's information age where the internet, social media in particular, is recognized as the most important modern public forum by our own Supreme Court.[48] This new public forum is truly global—not just American. Thus, it becomes extremely likely to have a "bleed-over" of U.S. government-created information entering this global public forum.[49] For this reason and greater transparency and accountability, the American public and government need different terms to refer to each type of activity. Put differently, the terminology must not inhibit an appreciation for the full effects of these different types of actions in the eyes of the government, the public, or the international community at large.

Finally, the ultimate means and ends of cyberspace and information operations are also mostly distinct.[50] Although information warfare might mainly use networks and systems to target people today, it does not have to and nor has it traditionally. Information warfare targets individual people and civil society generally, whereas cyber warfare targets networks and systems or underlying code that operates on those networks and systems. Information warfare also uses different tactics and techniques, such as utilizing social media, verse utilizing network or code-based vulnerabilities like cyber warfare. Admittedly, there may be some overlap in how these techniques work together, as well as a shared end goal of disrupting trust in systems, institutions, and people.[51] However, the overall differences between both operation types should

[48] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).

[49] *Cf.* U.S. ARMY WAR COLL., DEPT. OF MIL. STRAT., PLAN., AND OPERATIONS & CTR. FOR STRAT. LEADERSHIP, INFO. OPERATIONS PRIMER 12 (2011) (describing the difficulty in conducting information operations in the global information environment and describing restrictions implicated by the Smith-Mundt Act (1948) on government information influencing the American public).

[50] *But cf. generally*, Libicki, *supra* note 44.

[51] *See, e.g.*, KAPLAN, *supra* note 31, at 70 (describing the end goal of information [cyber] operations as getting the adversary to lose trust in their command and control); RICHARD M. CROWELL, WAR IN THE INFORMATION AGE: A PRIMER FOR CYBERSPACE OPERATIONS IN 21ST CENTURY WARFARE 16 (2010) (describing China as the "father of information warfare," listing the disruption of the enemy's cognitive system and its trust system as a main task).

outweigh a common title to fully inform the U.S. national consciousness about the true scope and effects of information warfare.

Thus, information warfare must be understood not as an offshoot of cybernetics or the access and control of networks, systems, or devices like cyber warfare. Rather, it is an offshoot of something far more ingrained in our collective history that is concerned with the access and control of people, directly targeting the cognitive. The next section builds on this notion and steers us in that direction.

2. Achieving Political Ends

The conduct of information warfare has roots much deeper than the 1970s and the advent of the internet. While advances in technology such as the internet and social media changed the means of engaging in information warfare and brought it to national attention, the long-established methods have not changed. This point is best illustrated through President Harry Truman's address on foreign policy in 1950 when addressing Communist propaganda, stating, "[d]eceit, distortion, and lies are systematically used by them as a matter of deliberate policy."[52] Truman's quote shows that information warfare tactics and their ends are far from new; in fact, it is well established that information warfare has been around for ages—even earlier than the 1950s. States used information warfare tactics in a range of military and government operations to protect and exploit the information environment dating back to the ancient Roman, Persian, and Chinese empires.[53]

The United States shares this storied history of conducting information warfare over the decades, albeit conducted under different monikers, such as psychological operations, foreign influence operations, or information operations.[54] The U.S. Office of Strategic Services, the precursor to the Central Intelligence Agency, for

[52] Harry S. Truman, Public Papers of the Presidents of the United States: Harry S. Truman 261 (vol. 6, 1950).
[53] Weedon et al., *supra* note 21, at 4; *see* Theohary, *supra* note 6.
[54] *See* Theohary, *supra* note 6.

example, used information warfare tactics during World War II to sow discord among enemy fighters and the Japanese public.[55] The United States also has an undeniably long history of using information warfare tactics to meddle in other countries' political matters and elections during peacetime.[56] Information warfare tactics used in the Cold War, the Iran-Contra affair, and the 1970 elections in Chile are but a few of these examples.[57]

Although a full retelling of the United States' history of covert intelligence and military information operations evades the scope of this article, it is enough to know that the traditional means and ends of information warfare have deep roots in U.S. history. What is worth going into more detail, however, is an early doctrine, titled "political warfare," that significantly influenced the nation's understanding of information warfare for the U.S. government.[58]

Against the backdrop of the looming Cold War and the enactment of the National Security Act of 1947, George Kennan, former State Department Policy Planning Director, [59] introduced the

[55] Buddhika B. Jayamaha & Jahara Matisek, *Social Media Warriors: Leveraging a New Battlespace*, 48 PARAMETERS: J. OF U.S. ARMY WAR C. 11, 13 (2019).
[56] *See* Peter Beinart, *The U.S. Needs to Face Up to Its Long History of Election Meddling*, THE ATLANTIC (July 22, 2018), https://www.theatlantic.com/ideas/archive/2018/07/the-us-has-a-long-history-of-election-meddling/565538/; *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee)*, bk. I, *Foreign and Military Intelligence*, 156-57, S. Rep. No. 94-755 (1976) (Church Comm. Rep.).
[57] *See Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee)*, bk. I, *Foreign and Military Intelligence*, 156, 490-91, S. Rep. No. 94-755 (1976) (Church Comm. Rep.); *see also* TAYACAN, PSYCHOLOGICAL OPERATION IN GUERILLA WARFARE § 5 (1984), https://www.cia.gov/library/readingroom/docs/CIA-RDP86M00886R001300010029-9.pdf.
[58] Kennan, *supra* note 42; *see also* Robinson et al., Modern Political Warfare: Current Practices and Possible Responses, RAND CORP., xix, 29 (2018), https://www.rand.org/pubs/research_reports/RR1772.html (defining information warfare as one of the key characteristics or methods of "political warfare").
[59] Kennan, *supra* note 42.

term "political warfare."[60] The term first appeared in a 1948 internal government document to describe what Kennan saw as the "inauguration" of an emerging type of warfare, although recognizing that the Government had already been engaged in such activities for some time.[61] In broadest terms, Kennan defined political warfare as "the employment of all the means at a nation's command, short of war, to achieve its national objectives."[62]

More specifically, Kennan concluded that such political warfare was "both overt and covert" and ranged from actions such as "political alliances, economic measures . . . , and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."[63] Kennan went on to recognize the Kremlin as the most refined and effective entity at using political warfare at the time,[64] feasibly a state of affairs unchanged today. Additionally, Kennan warned that the United States had been "handicapped . . . by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war . . . outside of all political context, . . . to seek [war as] a political cure-all . . . and . . . a reluctance to recognize the realities of international relations."[65]

Kennan's notion of political warfare should serve as a historical foundation for information warfare as it is the seed that grew our modern conception of the doctrine. At the outset, it is important to keep in mind that information warfare is but one part of the overall concept of political warfare, sharing the space and often overlapping with diplomatic operations, economic sanctions, or other deterrence

[60] *See id.*
[61] *Id.* at 1-2.
[62] *Id.* at 1.
[63] *Id.*
[64] *Id.*
[65] Kennan, *supra* note 42.

and influence efforts.[66] Accordingly, Kennan's political warfare primarily shapes our notion of information warfare by solidifying three major foundational concepts. First, Kennan confirms this type of warfare is about accessing people—in other words, targeting both society and decision-makers.[67] All of the activities cited by Kennan, such as overt propaganda, covertly influencing underground movements, or psychological operations, go to the heart of accessing people to influence them for some end goal.[68]

The second concept suggested by Kennan is that information warfare, as a subset of political warfare, is not, nor should it be, limited to wartime operations.[69] Arguably, its most potent form is deployed during peacetime, or below the threshold of armed conflict. In such cases, while there may not be overt hostilities or conventional fighting, there is most certainly a form of conflict.[70] Such was the case during the Cold War, as Kennan was watching it unveil.

The third concept is the suggestion by Kennan that the ends of this type of warfare should be to "achieve . . . national objectives."[71] This suggestion, however, requires further interrogation. The United States should not be so quick to adopt a definition for information warfare where the ends are described as achieving "national objectives." Time, unfortunately, has borne out the realities of information warfare and shown that it can be waged for reasons that do not comport with national objectives. Foreign and domestic non-

---

[66] *See generally* Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, RAND CORP., xix, 29 (2018), https://www.rand.org/pubs/research_reports/RR1772.html.

[67] *See generally id.*

[68] *See id.* at 3-5.

[69] *Id.* at 1. It is mainly for this reason that the old conception of information warfare put forward in the early 1990s fails to capture the true scope of information warfare, and likely why it no longer exists as a term within defense doctrine today.

[70] Crafting An Information Warfare and Counter-Propaganda Strategy For the Emerging Security Environment: Hearing Before the Subcomm. on Emerging Threats and Capabilities of the H. Comm. on Armed Serv., 115th Cong. 3 (2017) (opening statement of Hon. Elise M. Stefanik, N.Y. Rep., Chairwoman, Subcomm. on Emerging Threats and Capabilities).

[71] *See* Kennan, *supra* note 42.

state actors, as well as powerful national figures, have used information warfare to put forth their own group or individual interests, interests wholly divergent from national objectives.[72]

Thus, instead of looking to the exact language that Kennan proposed for the adoption of a national definition today, we should investigate its foundations further. Essentially, what Kennan proposed is what Carl von Clausewitz proposed centuries before—war is politics.[73] Clausewitz outlined two types of war: one to destroy an enemy as a political organism and one to take over territory.[74] Most serious students of war study Clausewitz; Kennan himself was no stranger. He cited Clausewitz in the opening sentence of his *Political Warfare* document and was inclined to view wars according to Clausewitz's classic dictum.[75] Hence, when we come to understand the ends of information warfare, we should go straight to Kennan's main point, which is that it is all about politics. The philosopher Aristotle argued centuries ago that, at our core, our capacity for reasoned speech is what makes us political animals.[76] Following this line of thought, information warfare targets reasoned speech as the primary means of attack and thus affects our politics. It is not just about achieving national objectives, but about achieving any political objectives.

That said, is information warfare actually "warfare"? This article answers this question in the affirmative. At the forefront of this conclusion is the fact that information warfare is most certainly a way of warfare today, or at a minimum, a great deal of how warfare is being conducted amid strategic competition. A secondary consideration is

[72] *See, e.g.*, Jarred Prier, *Commanding the Trend: Social Media as Information Warfare*, 11 STRATEGIC STUD. Q. 50, 63-67 (2017) (discussing the Islamic State's use of an information warfare campaign to advance its interests).
[73] Clausewitz's classic dictum is specifically stated as: "war is a mere continuation of policy by other means." CARL VON CLAUSEWITZ, ON WAR 87 (Michael Howard & Peter Paret eds., trans., Princeton University Press 1976).
[74] *See id.* at 22.
[75] DAVID MAYERS, GEORGE KENNAN: AND THE DILEMMAS OF US FOREIGN POLICY 123 (1990).
[76] Bernard Yack, *Community and Conflict in Aristotle's Political Philosophy*, 47 REV. OF POL. 92, 96 (1985).

that recognizing it as actual warfare may just require the United States to break out of a traditional Western mind frame. If the United States does not limit its collective understanding of warfare to armed conflict or warfare in the physical sense and instead understands it conceptually as a means to achieving political ends that can include nonphysical warfare, then this makes sense.[77] Sun Tzu advocates for this line of military thought, which is predominately followed by many adversarial states.[78] Thus, to think of warfare in the more limited sense, as only including the physical and bloodshed (admittedly, a historically predominate view), fails to take into account the state of international relations today,[79] a warning from Kennan that should be heeded.

The United States already witnessed the fallout from failing to recognize how adversarial states viewed warfare, in particular information warfare, and consequently failed to prepare the country for its impact. For example, the Kremlin openly discussed its position

[77] *See* Richard Davenport, *Know Thy Enemy*, ARMED FORCES J. (Sept. 1, 2009), http://armedforcesjournal.com/know-thy-enemy/; *see also* CROWELL, *supra* note 51, at 8-9.

[78] *See id.* Sun Tzu advocated for strategy aimed to achieve victory without battle: "to subdue the enemy without fighting is the acme of skill." GEOFFREY PARKER, THE CAMBRIDGE HISTORY OF WARFARE 1 (Geoffrey Parker ed., 2005).

[79] Both Russia and China, considered great power competitors to the United States in strategic competition, conceptualize information warfare as actual warfare. *See* CROWELL, *supra* note 51, at 8-9.; Davenport, *supra* note 73; Kennan, *supra* note 42; Prier, *supra* note 72, at 66-75 (noting "for Russia, information warfare is a specialized type of war, and modern tools make social media the weapon."); Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, RAND, 42-44 (2018), https://www.rand.org/pubs/research_reports/RR1772.html (describing Russia's view on information warfare as a subset of "new generation warfare," or political warfare, that Russia considers how warfare has evolved in general). *See generally* SOVIET INFLUENCE ACTIVITIES: A REPORT ON ACTIVE MEASURES AND PROPAGANDA, *supra* note 42; Crafting An Information Warfare and Counter-Propaganda Strategy For the Emerging Security Environment: Hearing Before Subcomm. on Emerging Threats and Capabilities of the H. Comm. on Armed Services, 115th Cong. 7 (2017) (statement of Timothy L. Thomas, Senior Analyst, Foreign Military Studies Office, Fort Leavenworth); Statement by Timothy L. Thomas Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, On Russia's Information War Concepts, 115th Cong. (2017).

on information warfare a year before the U.S. election interference.[80] The Kremlin's chief propagandist publicly stated in 2015, "information war is now the main type of war, preparing the way for military action."[81] Moreover, and perhaps most critically, limiting our understanding of information warfare to the physical will continue to blind the nation to the types of non-physical harm or violence that can result from this type of warfare.[82] A limited understanding of information warfare will greatly hamper society's collective ability to start reconceptualizing the real harms of the information age.

With this background in mind, information warfare should be conceived of as a type of strategic warfare as well as a method of warfare, conducted during times of both peace and war, ultimately aimed at destroying an enemy as a political organism through disruption or manipulation. This general aspect of information warfare, along with people as the target, remains constant no matter how many new means and methods emerge.

B. Means and Methods to Disrupt and Manipulate

1. Foundational Means and Methods

For context, it is important to briefly frame some of the foundational means and methods of information warfare before examining the changes brought about by the revolutionary information age.[83] The general types of information used in

[80] Peter Pomerantsev, *Inside Putin's Information War*, POLITICO (Jan. 4, 2015), https://www.politico.com/magazine/ story/2015/01/putin-russia-tv-113960.
[81] *Id.*
[82] *See* SAMULI HAATAJA, CYBER ATTACKS AND INTERNATIONAL LAW ON THE USE OF FORCE: THE TURN TO INFORMATION ETHICS, 54-62 (eds. Artur Gruszczak et al. 2019) (arguing for an informational approach to harm and violence). *See generally* Clare Sullivan, *The 2014 Sony Hack and the Role of International Law*, 8 J. NAT'L SEC. L. & POL'Y 437 (2016) (advocating for a different conception of harm in cyber-attacks, one that goes beyond physical consequences or is limited to the concept of harm in traditional warfare).
[83] Some might even call our current era an information or technical military revolution, the sixth revolution after the onset of the nuclear age. *See* Norman Davis,

information warfare include propaganda, disinformation, and misinformation.[84] The Russian interference in the 2016 U.S. presidential election (what can better be understood as disruption and manipulation) is likely one of the most recent, controversial, and highly publicized use of such information. The Russian disruption and manipulation of the U.S. election was mainly carried out using cyberspace and information warfare tactics, including extensive disinformation campaigns, with the strategic goal of sowing discord in the political system, thereby carried out for political ends.[85] And, to that end, it was historical and highly successful.[86]

An Information-Based Revolution in Military Affairs, 24 STRATEGIC REV. 43 (1996). *See generally* Christian Brose, *The New Revolution in Military Affairs*, 98 FOREIGN AFF. 122 (May/June 2019).

[84] Disinformation is the spreading of information which is knowingly false. *See* THEOHARY, *supra* note 6, at 5. In comparison, misinformation is the spreading of information that is unintentionally false. *Id.* at 5. Propaganda, on the other hand, is more of an idea or narrative intended to influence, which could include disinformation, misinformation, true information or even stolen information. *See id.* at 3, 5. In terms of the military, information warfare can be further divided into offensive and defensive information warfare operations. *See id.* at summary. Over the years, U.S. military doctrine conceptualized information warfare tactics that are related to these main types of information as including psychological operations and military deception operations, to name a few. *See id.* at 3. The distinguishing characteristics of these subsets of information operations rests mainly on who is targeted and who is carrying out the operations. *See generally id.*

[85] *See* Criminal Compl., *United States v. Internet Research Agency LLC*, ¶ 6, Case 1:18-cr-00032-DLF, Feb. 16, 2018. *See generally* Jonathan Masters, *Russia, Trump, and the 2016 Election,* COUNCIL ON FOREIGN RELATIONS (Feb. 26, 2018), https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election. According to an Oxford University report released on September 26, 2019, some 70 countries have had some type of disinformation campaign, either domestically or from foreign influence. Samantha Bradshaw & Philip N. Howard, *The Global Disinformation Order, 2019 Global Inventory of Organized Social Media Manipulation*, OXFORD INTERNET INST. (Sept. 26, 2019), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/ 93/2019/09/CyberTroop-Report19.pdf. The report shows that Governments are mainly spreading disinformation to "discredit political opponents, bury opposing views and interfere in foreign affairs."

[86] *See generally* Criminal Compl., *United States v. Internet Research Agency LLC*, ¶ 6, Case 1:18-cr-00032-DLF, Feb, 16, 2018. The 2016 election interference is historical and successful in that it caused the United States government to completely rethink

The success of Russia's covert information warfare operations over the last five years shows that there is likely no foreseeable end in sight.[87] Russia has increasingly turned to covert influence operations or "active measures" to achieve geopolitical aims.[88] "Such operations are not only more effective and cheaper than conventional military operations at weakening an opponent, but they have also resulted in far fewer international repercussions."[89] Thus, it is probably safe to say that the United States can only expect to see more of these disruptive and manipulative operations by Russia as well as other strategic competitors in the future.

Disruption and manipulation in other states' internal political matters is not a change in the practice of information warfare and typically received little public attention in years past.[90] Russia used information warfare to disrupt and manipulate multiple other elections around the world well before the 2016 U.S. elections.[91]

its national security posture and cause doubt about its security superiority over other nations, thereby shifting national security priorities. *See generally* S. REP. NO. 116-290, REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURE CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION; VOLUME 3: U.S. GOVERNMENT RESPONSE TO RUSSIAN ACTIVITIES (REDACTED) ("Senior U.S Government officials in both the Executive and Legislative Branches believed they were in unchartered territory in the second half of 2016."). *Cf.* U.S. DEP'T OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 2-3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[87] Michael Carpenter, *Countering Russia's Malign Influence Operations*, LAWFARE (May 29, 2019), https://www.justsecurity.org/64327/countering-russias-malign-influence-operations/.

[88] *Id.*; *see* Prier, *supra* note 72, at 66-75.

[89] Carpenter, *supra* note 87.

[90] *But cf.* Fletcher Schoen & Christoper Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major* Difference, 11 STRATEGIC PERSP. (2012), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf (examining a government interagency group that publicly exposed disinformation during the Cold War).

[91] Dana Priest, *Russian Disinformation on Facebook Targeted Ukraine Well Before the 2016 U.S. Election*, WASH. POST (Oct. 28, 2018), https://www.washingtonpost.com/business/economy/russian-disinformation-on-

Furthermore, and possibly more controversial, is the fact that the United States shared in this practice.[92] History bears out a rather long-established practice of states engaging in information warfare tactics in both wartime and peacetime, without much legal or international norm blockades to the practice.

That being said, no prior information warfare operations created the sort of domestic outcry that resulted after the 2016 U.S. election interference.[93] The debate around information warfare surged in recent years due to the role it played in political campaigns.[94] So, if information warfare is such an established practice, why then is there now overwhelming attention directed at stopping its harms? What has changed in light of such established practices? The answer to this question falls on the advent and surge of the platform economy and the rise of social media, which intensifies an adversary's ability to disrupt and manipulate, tipping actual harms even closer to destruction.

2. New Means and Methods: The Rise of Information Platforms and Social Media

The first mass proliferation of "fake news" enhanced by technology can trace its origins to the advent of the printing press. One of the first-ever mass-printed books on Britain's first printing press, *The Dictes and Sayings of the Philosophers*, was meant to compile the sayings of philosophers when in reality it was chock-full of fake news.[95] Radio and the television have also had their turn at facilitating

facebook-targeted-ukraine-well-before-the-2016-us-election/2018/10/28/cc38079a-d8aa-11e8-a10f-b51546b10756_story.html; Richard Forno, *Threats Remain to US Voting System – And Voters' Perceptions of Reality*, CEN. FOR INTERNET AND SOC'Y (Nov. 6, 2018), http://cyberlaw.stanford.edu/blog/2018/11/threats-remain-us-voting-system-%E2%80%93-and-voters%E2%80%99-perceptions-reality.

[92] *See* Beinart, *supra* note 56.

[93] *See, e.g.*, Blagovest Tashev & Brian McLaughlin, *Russia's Information Warfare: Exploring the Cognitive Dimension*, 10 MARINE CORPS UNIV. J. 129, 130 (2019).

[94] Brennen, *supra* note 25.

[95] ANDREW MARANTZ, ANTISOCIAL: ONLINE EXTREMISTS, TECHNO-UTOPIANS, AND THE HIJACKING OF THE AMERICAN CONVERSATION 65-66 (2019).

information warfare, and continue to do so today.[96] Yet, no change in technology rivals the meteoric rise of the information platform, in particular social media, and the resulting tectonic shift it caused in the practice, means, and methods of information warfare. Whereas other technological revolutions in the information age came on gradually, this one was fast and furious and arguably caught the world off guard.

The datafication, surveillance, and weaponization of everyday life is alarming and unprecedented.[97] Nonetheless, the extraction and exploitation of data, private surveillance of human activities, and the weaponization of civil society are quickly becoming the new normal for navigating the world as the nation shifts from an industrial-era economy into an emerging informational economy.[98] The technology that has made this shift in how we experience our world an inescapable reality is the information platform.[99]

Professor Julie Cohen defines the information platform as the new locus for market activities or a "site of encounter where interactions are materially and algorithmically intermediated."[100] Platforms employ multiple layers of technologies such as algorithms or computer protocols and machine intelligence. These technologies operate in concert to bound networks and infrastructures while simultaneously "making clusters of transactions and relationships stickier"—ultimately making it difficult for participants to exit.[101]

Platforms make up nearly all domains of human activity today. No information platform, though, highlights the ills of this

[96] *See, e.g.*, Pomerantsev, *supra* note 80.
[97] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 12 (2019) (suggesting surveillance capitalism is unprecedented in our times).
[98] *See id.*; JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 37 (2019).
[99] *See* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 89 (2016) (describing a "digital platform revolution," causing a "paradigmatic shift in the ways we produce, consume, work, finance, and learn").
[100] COHEN, *supra* note 98, at 37.
[101] *Id.* at 41.

emergent platform economy,[102] surveillance capitalism,[103] or the nascent "information war"[104] more than the social media platform. The social media platform prominently staked its claim on the everyday and often the most intimate social and communicative activity of billions of people worldwide.[105] Indeed, many have lauded social media's creation as a mechanism for cultural and political interconnection and collective action.[106] The Supreme Court even recently anointed social media as the new "modern public square."[107] But opposite these promising laurels comes an equally compelling dark side to this technology.

The rise of social media platforms upended society's previous understandings about the effects of information warfare. Social media effectively and efficiently allows adversarial actors engaging in information warfare tactics to target the spirit of the people.[108] Social media removes traditional barriers to manipulation and disruption, making it one of the most powerful tools available to adversaries to

[102] *See generally* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017) (suggesting the concept of the platform economy).
[103] *See generally* ZUBOFF, *supra* note 97 (suggesting the concept of surveillance capitalism). Professor Zuboff defines this concept primarily as a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales," or a "new global architecture of behavior modification" and "origin of new instrumentation power." *Id.* at Definition.
[104] *See generally* SINGER & EMERSON, *supra* note 42; RICHARD STENGEL, INFORMATION WARS (2019).
[105] Facebook alone connects over 2.2 billion people worldwide. VAIDHYANATHAN, *supra* note 20, at 10. As of 2019, the Pew Research Center estimated that seven-in-ten Americans use social media today to connect with one another, a statistic that has continued to exponentially grow over the past decade. *Social Media Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/social-media/.
[106] *See* COHEN, *supra* note 98, at 86-87 ("Networked, platform-based architectures enhance the ability to form groups and share information among members, to harness the wisdom and creativity of crowds, and to coalesce in passionate, powerful mobs."); *see generally* Lobel, *supra* note 99.
[107] Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).
[108] SINGER & EMERSON, *supra* note 42, at 18.

directly target civil society.[109] In other words, social media has made it simple to target or "weaponize" society, the likes of which have not been seen before.

The dark side of social media is driven by baked-in algorithmic mechanisms that allow for behavioral microtargeting and content optimization, which empirically creates intensified in-group effects or reinforces existing biases that are resistant to contradictory facts.[110] Put differently, platforms often use personal psychological profiles for targeting either for advertisements or content. This creates echo chambers and polarization that lead to a more destructive civil discourse by amplifying strong negative feelings about opposing views.[111]

While some argue that social media is simply a reflection of society, empirical studies indicate this is not a complete picture of reality. Studies show that social media exacerbates the effects of predisposed societal positions—it is not a mere reflection—and that there is a rightful concern raised about the breakdown of converged spaces of conversation and the extent of social media's effect in consolidating the boundaries between different groups.[112]

Fundamentally, one of the key problems with social media, summarized by Professor Eitan Hersh when testifying before Congress in 2018 about the future of data privacy, is that social media platforms like Facebook are inherently not made to be tools of the

[109] *Crafting An Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment: Hearing Before the H. Comm. On Armed Services*, 115th Cong. 3 (2017) (statement of Matthew Armstrong).
[110] COHEN, *supra* note 98, at 86-87.
[111] *See id.* at 87. Social media's ability to create "crowd-based judgments about the relevance, credibility, and urgency of online information . . . lend[s to] sensationalized, false, and hatred-inciting online material [with] extraordinary staying power . . . that cause both private and social harms."
[112] *See, e.g.*, Yong Jin Park et al., *Divide in Ferguson: Social Media, Social Context, and Division,* 4 SOC. MEDIA & SOC'Y 1, 11 (2018).

public forum intended to create an informed citizenship.[113] Social media platforms are instead designed to facilitate clicks and shares of content.[114] To do so, the kinds of news and content that are more readily supplied by platform algorithms is that which piques people's interest, and that which piques people's interest often appeals to their basest instincts; unfortunately, people are drawn to extremism, provocation, and outrage.[115] Then, when such effects are amplified due to platform affordances, the outcome is a very different and perhaps dark social discourse—one particularly ripe to be weaponized.

Further intensifying this problem is the fact that platform technology is meant to have another powerful psychological impact on addiction. Platform providers specifically create their platforms to be addictive.[116] Users then continue to come back and consume information from the platforms not just because they necessarily want to, rather they come back to engage because of some physiological subconscious draw. Hence, platform technology creates sticky situations on multiple levels.

C. Understanding and Rethinking Information Warfare Harms

The emergence of new means and methods of information warfare warrant a brief examination and rethinking of the types of associated harm. Do advanced and more dangerous means and methods lead to new forms of harm; is it beyond disruption and manipulation of the individual, or beyond the destruction of a nation or political organism? How government and society conceive of

---

[113] *Cambridge Analytica and the Future of Data Privacy: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 8 (2018) (statement of Eitan Hersh, Professor, Tufts University).
[114] *Id.* at 8.
[115] *Id.* at 7.
[116] SINGER & EMERSON, *supra* note 42, at 3; *see* Trevor Haynes, *Dopamine, Smartphones & You: A Battle For Your Time*, HARVARD.EDU (May 1, 2018), http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/. *See generally* Diana I. Tamir & Jason P. Mitchell, *Disclosing information about the self is intrinsically rewarding*, 109 PROC. NATL ACAD. SCI. U.S.A. 8038 (2012); Daria J. Kuss & Mark D. Griffiths, *Online social networking and addiction--a review of the psychological literature*, 8 INT'L J. ENV'T RES. & PUB. HEALTH 3528 (2011).

information warfare harms ultimately drives the application and relevance of U.S. domestic laws (as well as international laws and norms).

Social media has unmistakably become a new hotbed for information warfare and its resulting harms. Some scholars labeled the harm from the 2016 U.S. election interference on social media an "attack on the integrity of the U.S. political system."[117] And while the United States predominately focused on election interference over the past five years, the U.S. government overlooked a more virulent information warfare campaign: Russia's information warfare campaign targeting the anti-vaccination debate. Failing to address this campaign allowed it to gain traction and reap potentially devasting effects that could linger for years to come. In the wake of the 2019 novel coronavirus (COVID-19) pandemic, this is even more concerning.

Russia waged a global information warfare campaign on social media for many years against the discourse surrounding vaccinations. The campaign was discovered in late 2018 by a team of researchers studying ways to improve social media communications for public health workers.[118] The study discovered several Russian trolls and bots, some being the same that interfered in the U.S. election, spread misinformation and disinformation online about vaccinations since at least 2014.[119] According to the study, Russian trolls and bots were found to be significantly more likely to contribute to the debate and divisive messaging than other actual platform users.[120] The results also

[117] Max Boot and Max Bergmann, *Defending America From Foreign Election Interference*, COUNCIL ON FOREIGN REL. (March 6, 2019), https://www.cfr.org/report/defending-america-foreign-election-interference.
[118] Jessica Glenza, *Russian Trolls 'Spreading Discord' Over Vaccine Safety Online,* THE GUARDIAN (Aug. 23, 2018), https://www.theguardian.com/society/2018/aug/23/russian-trolls-spread-vaccine-misinformation-on-twitter.
[119] Broniatowski et al., *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*, 108 AM. J. OF PUB. HEALTH 1378, 1378 (2018).
[120] *See id.* at 1379-80.

showed that proportions of polarized and anti-vaccine messages devised by trolls and bots far exceeded actual users, and the messages themselves were significantly more polarizing.[121] The study concluded that these posts were responsible for eroding public consensus on vaccination.[122] The lead researcher warned that these information warfare campaigns waged on social media took what was once a fringe opinion on vaccination and turned it into a transnational movement.[123]

Russia's targeting of the anti-vaccination debate on social media should come as no surprise, though. Adversarial actors target a whole host of divisive topics within civil society, not just geopolitics and military operations. On a global scale, topics that malicious actors use to create societal divisions and sow discontent range from politics, religion, culture, race, environment, diet, and health.[124] Presently, the Kremlin and other adversarial states to the United States may be engaging in significant disinformation campaigns regarding COVID-19.[125] Polarizing topics such as these are targeted because they have the

[121] *See id.* at 1380-81.

[122] Lia Eustachewich, *Russian Trolls Blamed for Spreading Anti-Vaccination Propaganda*, N.Y. POST (Feb. 15, 2019), https://nypost.com/2019/02/15/russian-trolls-blamed-for-spreading-anti-vaccination-propaganda/.

[123] Talha Burki, *Vaccine Misinformation and Social Media*, 1 THE LANCET 258, 258 (2019), https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30136-0/fulltext (citing David Broniatowski).

[124] *See* Bessi et al., *Trend of Narratives in the Age of Misinformation*, 10 PLOS ONE 1, 1 (2015); *see, e.g.*, Julia Ioffe, *The History of Russian Involvement in America's Race Wars*, ATL. (Oct. 21, 2017), https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/; Robin Emmott, *Russia Deploying Coronavirus Disinformation to Sow Panic in West EU Document Say*, REUTERS (Mar. 18, 2020), https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F.

[125] Gary Corn, *Coronavirus Disinformation and the Need for States to Shore Up International Law*, LAWFARE (Apr. 2, 2020), https://www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law; *see also* Jack Murphy, *Can the State Dept. Lead America's Effort to Fight COVID-19 Disinformation?*, RADIO.COM (Apr. 2, 2020), https://connectingvets.radio.com/articles/global-engagement-center-seeks-to-combat-covid-disinfo.

best potential to divide a nation or political entity by simply amplifying cleavages.[126]

Most of these topics like health security—dwarfed in the limelight of election interference—received little to no attention from domestic decision-makers, until perhaps recently.[127] Given the current state of information warfare, our legal framework, and the current global pandemic, this inattention can be a truly fatal mistake. There is a good case that this topic alone creates more harm than any other topic targeted, including everything from election interference to terrorism.[128]

Similar to election interference, spreading disinformation about vaccinations works toward political ends; it has the potential to undermine the nation's healthcare system and its national security by sowing unrest and creating distrust of government. In stark contrast, unlike election interference, health disinformation can lead to direct

---

[126] *See* Bessi et al., *supra* note 124; Carpenter, *supra* note 87.

[127] To be fair, small pockets of the U.S. government attempt to address disinformation surrounding public health issues. *See, e.g.*, Melissa Jenco, *Health Officials Combating Measles Vaccine Misinformation as Cases Reach 1,001*, AAP NEWS (June 6, 2019), https://www.aappublications.org/news/2019/06/06/measles060619. The Global Engagement Center (GEC), the State Department agency tagged with serving as the center for combating disinformation campaigns, acknowledged efforts were needed to combat the recent disinformation campaigns surrounding the COVID-19 pandemic. Jack Murphy, *Can the State Dept. Lead America's Effort to Fight COVID-19 Disinformation?*, RADIO.COM (Apr. 2, 2020), https://connectingvets.radio.com/articles/global-engagement-center-seeks-to-combat-covid-disinfo.

[128] *Compare* Hannah Ritchie et al., *Terrorism*, OUR WORLD IN DATA (Nov. 2019), https://ourworldindata.org/terrorism *with* Nsikan Akpan & Vanessa Dennis, *How Bad is the Measles Comeback? Here's 70 Years of Data*, PBS (June 18, 2019), https://www.pbs.org/newshour/science/how-bad-is-the-measles-comeback-heres-70-years-of-data. *See also* Sabrina Siddiqui, *Half of Americans See Fake News As a Bigger Threat Than Terrorism, Study Says*, THE GUARDIAN (June 7, 2019), https://www.theguardian.com/us-news/2019/jun/06/fake-news-how-misinformation-became-the-new-front-in-us-political-warfare ("[A Pew Research Center Study concluded] half of Americans view fake news as a bigger threat to the country than terrorism, illegal immigration, violent crime or racism.").

harm to people and worldwide health security risks.[129] By eroding public trust in vaccinations to promote discord in civil society, these information operations expose people—on a global scale—to the risk of infectious diseases and direct physical harm.[130] Direct harm to the global population is even more likely when coupling information campaigns aimed at eroding trust in vaccinations with eroding trust in a nation's healthcare system and ability to effectively respond to a deadly virus.[131] In the end, "viruses do not respect national boundaries,"[132] and increasingly, neither does information. Unfortunately, proof of this adage is ever-present today with the COVID-19 pandemic.

To envision a future where information warfare tactics targeting public health go unaddressed, the United States should look to the 2018 measles epidemic in Europe, which provides proof of how this type of campaign can lead to dire consequences.[133] The European measles epidemic serves as a good case study because it was the first epidemic ever publicly recognized as largely being driven by disinformation and misinformation campaigns on social media, such as the one carried out by Russia.[134] European leaders specifically

[129] *See, e.g.*, Corn, *supra* note 125.
[130] The George Washington Univ., *Russian Trolls, Bots Influence Vaccine Discussion on Twitter,* GW TODAY (Aug. 24, 2018), https://gwtoday.gwu.edu/russian-trolls-bots-influence-vaccine-discussion-twitter (quoting Mark Dredze, professor of computer science at Johns Hopkins).
[131] *See* Corn, *supra* note 125.
[132] The George Washington Univ., *supra* note 130.
[133] *See* Abdi Latif Dahir, *Measles Cases Continue to Rise Around the World*, N.Y. TIMES (Nov. 26, 2019), https://www.nytimes.com/2019/11/26/health/measles-outbreak-epidemic.html; Ron Synovitz, *Are Russian Trolls Saving Measles From Extinction?*, RADIO FREE EUROPE, RADIO LIBERTY (Feb. 13, 2019), https://www.rferl.org/a/are-russian-trolls-saving-measles-from-extinction/29768471.html; Sabrina Sidhu, *Alarming Global Surge of Measles Cases a Growing Threat to Children-UNICEF*, UNICEF (Feb. 28, 2019), https://www.unicef.org/press-releases/alarming-global-surge-measles-cases-growing-threat-children-unicef-0.
[134] *See, e.g.*, Ellen Coyne, *Social Media Undermines Vaccinations, Warns Harris,* THE SUNDAY TIMES (London) (Dec. 7, 2018), https://www.thetimes.co.uk/article/social-media-undermines-vaccinations-warns-harris-d8l70rkht. *See also* Chris Green,

blamed such campaigns as causing the epidemic to grow due to overall vaccine hesitancy, an issue rising worldwide.[135] At least for the United Kingdom, this acknowledgment also came in the wake of it losing its measles-free status last year by the World Health Organization.[136] Subsequently, the United Kingdom, its country neighbors, international organizations, and some platform providers spurred into action to address this threat abroad.[137]

Falling Children's Vaccination Rates Blamed on Social Media 'Pseudoscience', iNEWS (Scotland) (Mar. 26, 2019), https://inews.co.uk/news/scotland/falling-childrens-vaccination-rates-blamed-on-social-media-pseudoscience-504818; Mike Hill, *Lancashire's Low MMR Vaccination Rate Blamed on Social Media*, LANCASHIRE POST (London) (Mar. 15, 2019), https://www.lep.co.uk/news/latest/lancashire-s-low-mmr-vaccination-rate-blamed-on-social-media-1-9652849. A recent UNICEF publication went so far as to say, "measles may be the disease, but, all too often, the real infection is misinformation." Sidhu, *supra* note 133. A European study published last year found that the prevailing disinformation messages on social media surrounded the Measles, Mumps, and Rubella (MMR) vaccine. *See* Steffens et al., *How Organizations Promoting Vaccination Respond to Misinformation on Social Media: A Qualitative Investigation,* BMC PUB. HEALTH, 19:1348, 4 (2019), https://bmcpublichealth. biomedcentral.com/articles/10.1186/s12889-019-7659-3. The largest global study on immunization attitudes, The Wellcome Trust Analysis, highlighted in 2018 the fact that Russian interference in the antivaccination debate on social media likely bolstered vaccine hesitancy. GALLUP WELLCOME GLOBAL MONITOR – FIRST WAVE FINDINGS, HOW DOES THE WORLD FEEL ABOUT SCIENCE AND HEALTH?, 119 (2019), https://wellcome.ac.uk/ sites/default/files/wellcome-global-monitor-2018.pdf.

[135] A 2019 British health survey cites to social media disinformation as one of the three main influences for vaccine hesitancy. ROYAL SOCIETY FOR PUBLIC HEALTH, MOVING THE NEEDLE: PROMOTING VACCINATION UPTAKE ACROSS THE LIFE COURSE 3 (2018), https://www.rsph.org.uk/uploads/assets/uploaded/3b82db00-a7ef-494c-85451e78ce18a779.pdf.

[136] Nick Bostock, *GPs Urged to Promote MMR Catch-Up as U.K. Loses 'Measles-Free' Status*, GP (Aug. 19, 2019), https://www.gponline.com/gps-urged-promote-mmr-catch-up-uk-loses-measles-free-status/article/1594176.

[137] The United Kingdom proposed tough laws that require major platforms to remove disinformation and harmful content from their sites. Ryan Browne, *The UK is Going After Big Tech for Harmful Content: Here's Why it Matters*, CNBC (Apr. 8, 2019), https://www.cnbc.com/2019/04/08/the-uk-is-going-after-big-tech-over-harmful-content.html. Within the last year, before the outbreak of COVID-19, many countries and organizations made concerted efforts to denounce the targeting of vaccination debates online. *See, e.g.*, Michelle Roberts, *Vaccines: Low Trust in*

We also look to the information warfare campaigns targeting the anti-vaccination debate surrounding the measles epidemic because the virus is extremely contagious—more so than Ebola, tuberculosis, or influenza.[138] Once infected, there is no specific treatment for measles, so vaccination is a critical life-saving tool, especially for children.[139] Over the last two decades, the measles vaccination has prevented over 21.1 million deaths.[140] Deaths from measles now range over 100,000 per year, but these numbers are steadily rising due to increasing gaps in vaccination coverage,[141] propelled in large part by social media information warfare campaigns. Although these numbers seem minimal in light of COVID-19 fatalities, listing out these statistics underscores the foreseeability of fatalities caused by known information operations that target society with health disinformation.

The measles statistics also expose a critical oversight in cyber and information harms, as well as corresponding norm building. Many legal scholars and experts claim that deaths either rarely or have

Vaccination 'A Global Crisis', BBC NEWS (June 19, 2019), https://www.bbc.com/news/health-48512923 (citing The World Health Organization as recently listing vaccine hesitance as one of the top global health threats); Elaine Loughlin, *Harris to Meet Social Media Firms to Stop 'Downright Lies' by Anti-Vaccination Groups*, IRISH EXAMINER (Aug. 28, 2019), https://www.irishexaminer.com/ breakingnews/ireland/harris-to-meet-social-media-firms-to-stop-downright-lies-by-anti-vaccination-groups-946671.html. Some countries, such as France, even increased mandatory vaccination laws. Alex Whiting, *How France is persuading its Citizens to Get Vaccinated*, CNN (Nov. 5, 2019), https://www.cnn.com/2019/07/03/health/france-fighting-vaccine-skepticism-partner-intl/index.html. Many platforms in response changed their terms of service to filter, discredit, or demonetize anti-vaccination content. *See, e.g.*, Katie Notopoulos, *Instagram Will Use AI To Filter Anti-Vax Content*, BUZZFEED NEWS (May 7, 2019), https://www.buzzfeednews.com/article/katienotopoulos/instagram-will-use-ai-to-filter-anti-vax-content.

[138] Sidhu, *supra* note 133. The United Kingdom became a clear leader in these international efforts. In August 2019, for example, the British Prime Minister outlined plans for a summit of social media firms to discuss how to promote accurate information about vaccinations. Burki, *supra* note 123.

[139] *Id.*

[140] CTR. FOR DISEASE CONTROL, MEASLES DATA AND STATISTICS, 1-2 (Apr. 16, 2019), https://www.cdc.gov/measles/downloads/MeaslesDataAndStatsSlideSet.pdf.

[141] *See id.*; *See also* Dahir, *supra* note 133.

never directly resulted from a cyber or information operation,[142] alluding to the notion that such operations do not result in physical harms, most often viewed as the threshold requirement for an illegal attack under international law.[143] These claims then tend to facilitate the continuation of information warfare tactics by states because such state action is accordingly viewed as operating within the bounds of international and domestic laws and, thus, likely to result in little to no justifiable consequences on the international stage.[144]

In a very narrow sense, these claims are true. At the same time, however, these claims regarding the nature and consequences of harm do not fully comport with a domestic or international legal understanding of harms. Under either framework, liability can attach to bad actors for foreseeable or anticipated as well as direct harms, a notion often overlooked.[145] The statistics discussed above as they relate

[142] Steven Feldstein & David Sullivan, *Protecting Civilians in Cyberspace: Ideas for the Road Ahead*, LAWFARE (July 3, 2018), https://www.justsecurity.org/58838/protecting-civilians-cyberspace-ideas-road/; DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBERAGE, xi (2018); Libicki, *supra* note 44, at 55.

[143] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, Rule 82 & 92 (Michael N. Schmitt ed., 2 ed., 2017) [hereinafter *Manual*]; *see also* Helen Durham, *Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions*, ICRC (blog) (Mar. 26, 2020), https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/ (discussing when international humanitarian law is thought to apply to cyberspace operations).

[144] *Manual, supra* note 143, at Rule 82, 92. Generally speaking, under the current state of the law, cyber-attacks "causing the same or similar effects as those that would be considered a use of force if caused through traditional physical means" amount to an "armed attack." Non-destructive actions typically do not rise to the level of an armed attack, although some scholars assert that actions that impair state functionality and stability could qualify as a use of force or armed attack. *See id.* For further discussion on norm development and the international legal framework governing cyber and information warfare operations and the challenges in defining harm in a law of armed conflict and international law paradigm, *see* HAATAJA, *supra* note 82, at 2-6.

[145] Under international humanitarian law, an attack is prohibited if it is foreseeable that the damage to the civilian population will be in excess to the military advantage gained; this is the principle of proportionality. Further, some scholars have recently

to measles, and likely more so with COVID-19, challenge whether the harm analysis should stop at only those direct harms when such harms caused by health disinformation are entirely foreseeable—both to the type of injury and general class of people.[146] The cyber information warfare operations targeting the anti-vaccination debate directly led to large gaps in vaccinations—a foreseeable result of this type of information warfare campaign—which is attributable to the foreseeable deaths that could have been prevented. When looking at this problem as a holistic worldwide problem, rather than one focused solely on individualized direct harm, it becomes hard to argue against the notion that this type of information warfare campaign causes legally cognizable harm—specifically, fatalities.[147]

Focusing on individual harm rather than the public's harm more generally also fails to match how we focus on collective public advantages to information platforms (our new speech market) and data collection and surveillance, which facilitates information harms. Thus, to correct this disparity, we should make more symmetrical policy arguments for reform and compare those public advantages to the greater public harm (i.e., global fatalities, increasing national

started to argue that information or cyber warfare is a direct harm inflicted on a state as an informational entity, causing some damage or destruction as an entity thus impacting its very being and right to exist. HAATAJA, *supra* note 82, at 59. Similarly, under domestic law, liability can also attach for foreseeable harms, not merely direct harms, which is an age-old principle of the law of torts— "there is no liability unless the harm produced was, in some measure, to be anticipated." Fowler Vincent Harper, *Foreseeability Factor in the Law of Torts,* 7 NOTRE DAME L. REV. 468, 469 (1932).

[146] Given that operations are carried out in a targeted manner using social media platforms, it becomes even more plausible to state that the type of harm and general class of persons to be harmed is foreseeable, requirements under a domestic tort liability analysis. *See* Harper, *supra* note 145, at 470. A similar analysis is conducted within the principle of proportionality for international humanitarian law as well.

[147] Vaccines are critical for the global population's health security because they help establish herd immunity which usually requires immunity for 70% to 90% of a population. Gypsyamber D'Souza & David Dowdy, *What is Herd Immunity and How Can We Achieve it With COVID-19?*, JOHN HOPKINS BLOOMBERG SCH. PUB. HEALTH (Apr. 10, 2020), https://www.jhsph.edu/covid-19/articles/achieving-herd-immunity-with-covid19.html.

security risks, and the deterioration of our democracy) rather than merely individual harm.[148]

Although not quite there yet, the United States needs to at least start reconceptualizing harm as not only those direct and immediate impacts but also foreseeable or anticipated collective harms that are maliciously intended by bad actors. At the very least, these information operations exemplify that "distinctions between offline and online conflicts are blurring as tools and tactics deployed in cyberspace trigger real world consequences."[149] People are starting to see this play out in their daily lives. Robert Califf, the former commissioner of the U.S. Food and Drug Administration, warned years ago that medical misinformation and disinformation is "the issue of our times that demands top priority."[150] He posited this well before COVID-19 came into existence and fueled information warfare campaigns, of which now range from disinformation about the severity of the virus, potential cures, and the efficacy of vaccinations.[151] Many experts and studies are beginning to reveal that disinformation

[148] *See* LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 88 (2020).
[149] Feldstein & Sullivan, *supra* note 142.
[150] Synovitz, *supra* note 133.
[151] *See* Lauren Feiner, *Democratic Senators Urge Facebook, Google and Twitter to Crack Down on Vaccine Misinformation*, CNBC (Jan. 25, 2021), https://www.cnbc.com/2021/01/22/facebook-google-and-twitter-urged-by-senators-to-crack-down-on-vaccine-misinformation.html; Sheera Frenkel, et al., *Surge of Virus Misinformation Stumps Facebook and Twitter*, N.Y. TIMES (Mar. 8, 2020), https://www.nytimes.com/2020/03/08/technology/coronavirus-misinformation-social-media.html; Jessica Guynn & Aleszu Bajak, *We Are Talking About People's Lives': Dire Warnings of Public Health Crisis as COVID19 Misinformation Rages*, USA TODAY (Dec. 9, 2020), https://www.usatoday.com/story/tech/2020/12/09/coronavirus-vaccine-misinformation-facebook-twitter-youtube/3867707001/; Davey Alba & Sheera Frenkel, *Misinformation Messengers Pivot from Election Fraud to Peddling Vaccine Conspiracy Theories*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/us/misinformation-messengers-pivot-from-election-fraud-to-peddling-vaccine-conspiracy-theories.html.

about COVID-19 needlessly intensified the deadly public health crisis and continues to do so.[152]

Lives are at stake. There is no better time than now to make it a national priority to determine how U.S. laws can help facilitate, rather than hamper, the fight against information warfare and perhaps start to reframe our concept of harm. The U.S. government and private sector must come together to examine how laws and regulations can appropriately control and protect that access to people to ensure that they are not maliciously targeted for political ends. Primarily, this requires a focus on the domestic legal framework surrounding content or speech and reexamining the confines of the First Amendment.

III. CONTENT (SPEECH)

The challenges of the First Amendment lead some scholars to the rather radical, yet entirely fair, conclusion that "Congress may need to restrict the freedom of speech of Americans" to combat information harms like information warfare.[153] Driving this assertion is a general perception that an immutable paradox exists between protecting the freedom of speech for individuals and information platforms on one side, and the ability of government to address information harms such as the protection of national security interests and the deterioration of individual privacy and democratic institutions on the other side.[154] Rather than jumping to extraordinary conclusions about solutions, it seems more prudent to further explore the scope of the First Amendment, and reconceptualize its animating ideals and jurisprudence in light of the rise of information and social

[152] *See, e.g.*, Christopher Ingraham, *New research explores how conservative media misinformation may have intensified the severity of the pandemic*, WASH. POST (June 25, 2020), https://www.washingtonpost.com/business/2020/06/25/fox-news-hannity-coronavirus-misinformation/ (citing multiple research studies concluding COVID-19 misinformation led to increased harm or deaths); Alison Coleman, *'Hundreds dead' because of COVID-19 misinformation*, BBC (Aug. 12, 2020), https://www.bbc.com/news/world-53755067.

[153] Goldenziel & Cheema, *supra* note 5, at 87.

[154] *Cf.* Goldsmith, *supra* note 14 (advocating similar views but framing the issue in terms of the United States' "internet freedom" model of governance). *See generally* Goldenziel & Cheema, *supra* note 5, at 87.

media platforms—the new marketplace of ideas. This exercise illuminates that what many accepted in the past as the contours of the freedom of speech and governments' related duties to protect this right now fail to promote underlying First Amendment values within a platform economy that allows information warfare to flourish. Our unique domestic law challenges may not, after all, lie with the First Amendment itself.

A. Reexamining the "Market" and Government Regulation

1. The Regulatory Void

The precarious new platform "market" that was discussed in Part II.B.2 suggests the need for government to implement significant laws and regulations to govern and stabilize this environment for consumers and businesses. To present, quite the opposite has been the case. The platform economy has exponentially grown within a substantially deregulated environment driven by a market and legal ideology that values innovation, technology growth, and near-peer competition over individual privacy, security, and often, as a consequence, democratic ideals.[155]

Two laws, in particular, played a large role in creating this substantial regulatory void. The first, the Communications Decency Act (CDA), Section 230, was enacted as part of the Communications Act overhaul under the Telecommunications Act of 1996 that primarily aimed to promote competition and reduce regulation in telecommunications.[156] Section 230 was enacted to protect providers

[155] *See* Cohen, *supra* note 98, at 191-92; *see also id.* at n.79*; see also Cambridge Analytica and the Future of Data Privacy: Statement of Mark Jamison Before the S. Judiciary Comm., Politics and Business in Social Media*, 115th Cong. 7-8 (statement of Mark A. Jamison, Ph.D., Visiting Scholar, American Enterprise Institute) (discussing how regulations place on firms, such as social media, stifle innovation and competition). *See generally* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639 (2014); Goldenziel & Cheema, *supra* note 5 (arguing that U.S. Laws must be reformed concerning speech, information and privacy to protect the democratic process and national security).

[156] *See* Telecommunications Act of 1996, P.L. No. 104-104, 110 Stat. 56 (1996).

of an interactive computer service from civil liability for another's actions.[157] Over the years, courts interpreted platform companies as interactive computer service providers who can benefit from the liability shield of the CDA; thus, forcing regulators to look elsewhere to regulate the platforms themselves.[158] Now, with platform information harms, such as information warfare campaigns and persistent commercial surveillance, coming to the forefront of the national consciousness, many scholars and policymakers advocate for amending CDA Section 230 as a solution.[159]

The second law, and focus here, that plays an even more significant role in the creation of the light-touch regulatory framework for platforms—and is seemingly far more of a challenge to address than Section 230—is the First Amendment.[160] In the most basic terms applicable to platforms, the doctrine prohibits the government from foreclosing access to a public forum[161] and censoring a speaker's ability to give or a listener's ability to receive speech or information, but for extremely limited circumstances.[162] Additionally, it protects the related doctrine of association.[163] The recent development of commercial speech jurisprudence within the First Amendment framework also plays a role in protecting certain marketing or advertising techniques that underpin platforms' business models as a

[157] Lobel, *supra* note 99, at 144.
[158] *See id.* at 146.
[159] *See, e.g.*, STENGEL, *supra* note 104, at 294-95.
[160] *See* Cohen, *supra* note 98, at 162 ("The legal construction of platform immunity for information harms is in part a constitutional strategy that leverages preexisting trends in first amendment jurisprudence.").
[161] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017); *see, e.g.*, Police Department of Chicago v. Mosley, 408 U.S. 92 (1972).
[162] *See, e.g.*, Citizens United v. FEC, 558 U.S. 310 (2010).
[163] *See, e.g.*, NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460 (1958); *see also* Hans Allhoff, *Membership and Messages: The (Il)logic of Expressive Association Doctrine*, 15 J. CONST. L. 1455, 1462-63 (2013).

form of speech.[164] Both individuals and platform providers claim these First Amendment protections for their platform activities.[165]

As a result of these protections and their assumed application, platform providers can rely on the First Amendment to "craft narratives that make unaccountability for certain types of information harms seem logical, inevitable, and right."[166] Hence, a forceful narrative emerged to shield information and social media platforms from government regulation and oversight regarding information warfare. This narrative is what the remaining sections begin to dismantle.

2. A Functioning Marketplace?

One of the main conceptual cornerstones of the First Amendment tradition comes from Justice Holmes dissenting in *Abrams v. United States*, where he conceptualized the First Amendment in terms of the public sphere serving as a marketplace of ideas.[167] To reconceptualize First Amendment doctrine, one must first question whether this marketplace of ideas is even functioning, as it was originally conceived by Holmes, in the context of social media platforms—the new speech market. Justice Holmes meant for his "marketplace of ideas" to be a part of the great experiment that is our

[164] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011).
[165] *See, e.g.*, Cohen, *supra* note 98, at 167 (discussing platforms ability to claim expressive immunity under the First Amendment). In *Reno v. ACLU*, the Supreme Court established that online speech receives the same First Amendment protections as other forms of speech. 521 U.S. 844, 870 (1997).
[166] Cohen, *supra* note 98, at 161.
[167] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("that the ultimate good desired is better reached by free trade in ides - that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . ."). For further background on how Justice Holmes dramatically shifted the trajectory of First Amendment jurisprudence from his opinions in the 1919 Espionage Act cases to the 1919 *Abrams* case in less than a year, *see*, THOMAS HEALY, THE GREAT DISSENT: HOW OLIVER WENDELL HOLMES CHANGED HIS MIND—AND CHANGED THE HISTORY OF FREE SPEECH IN AMERICA (2014).

Constitution,[168] one that allows our ideas about it to be tested, studied, and perhaps altered over time.

In the early 2000s before the dawn of social media and the platform economy boom, the assertion that "[t]he advent of the internet may have moved society closer to the ideal Justice Brennan outlined in *New York Times Co. v. Sullivan* by making the debate on public issues more 'uninhibited, robust, and wide-open'"[169] could hardly be countered.[170] Ironically, however, that notion is highly debatable now when put up against the new speech market of social media platforms, of which have been singled out by the Supreme Court as the most important place for the exchange of views,[171] virtually replacing the quintessential "public streets and parks"[172] as the new modern public square.

While there is no doubt that far more information swarms within our information environment today than ever before—these are not, the days of true informational scarcity—[173] there is still far less than the majority of Americans might consume, be exposed to, or collaborate on in the age of information platforms. Remember, platforms are created to be sticky; providers strive to keep users within their interface to drive their business model where user data is the raw

[168] *See Abrams*, 250 U.S. at 630 (Holmes, J., dissenting).
[169] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).
[170] Bernard W. Bell, *Filth, Filtering, and the First Amendment: Ruminations on Public Libraries' Use of Internet Filtering Software*, 53 FED. COMM. L.J. 191 (2001).
[171] To be clear, the Supreme Court in *Packingham* identified the most important place (in a spatial sense) for the exchange of views today to be "cyberspace . . . and social media in particular." Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).
[172] *See Packingham*, 137 S. Ct. at 1738 (Alito, J., concurring); *see, e.g.*, Pleasant Grove City v. Summum, 555 U.S. 460, 469 (2009).
[173] *See* Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 553 (2018). Professor Wu compares speakers today to moths: "their supply is apparently endless, and they tend to congregate on brightly lit matters of public controversy." *Id.* at 549. Arguably, Professor Wu's analogy is only highlighting one aspect of the psychological control of information platforms. When looking at the problem holistically, it is not entirely about user choice when users stay within their information bubbles or echo-chambers, even though they might have initially been drawn there by the "brightly lit matters of public controversy."

material to be collected and exploited.[174] Platforms have no duty to their users to protect channels of communication,[175] as perhaps the government might.[176] Rather, platforms have a fiduciary duty to stakeholders to profit from their business model.[177] Under the current pervasive surveillance and datafication business model of platforms,[178] it is not in the interests of platforms and their stakeholders "to protect the main channels of expression;"[179] it is in their interest to close those channels, keeping users pigeonholed by remaining hyper-focused on content that draws users.[180] In essence, silencing or controlling outside speakers is the name of the game.

Platforms achieve these goals by microtargeting information and creating unprecedented psychological effects that lead to the resistance of contradictory facts and the creation of echo chambers.[181]

---

[174] Facebook often asserts that it does not sell its data; however, it is still very much in the business of data exploitation. Facebook collects its user's data to create psychological profiles, which it then sells access to for third party advertisers, who then use those opportunities to collect their own data on users. In sum, data is advertising, and advertising is data in today's platform economy. For insight into Facebook's business model, *see* AMELIA ACKER, DATA CRAFT: THE MANIPULATION OF SOCIAL MEDIA METADATA 20 (2018), https://datasociety.net/library/data-craft/.

[175] *See generally* Lina Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 508-09 (2019) (arguing that platforms only have a duty to their shareholders).

[176] *See generally* Wu, *supra* note 173.

[177] Khan & Pozen, *supra* note 175, at 508-09.

[178] For a discussion on the development of the platform business model, *see* Cohen, *supra* note 98 at 141-43.

[179] David A. Graham, *The Age of Reverse Censorship*, THE ATLANTIC (Jun. 26, 2018) (citing Professor Wu).

[180] See discussion in Part II.B.2.

[181] *See* Cohen, *supra* note 98, at 86-87; *cf.* Wu, *supra* note 173, at 555 (referring to this psychological phenomenon as the rise of the "attention industry" – a business model framed on the resale of human attention – and the "filter bubble"). Strikingly, the most severe effects of social media microtargeting and the development of in-groups might be comparable to those methods of coercion espoused by Albert Biderman in 1973, who investigated the treatment of prisoners of war for Amnesty International. *See* Rus Ervin Funk, *Biderman's Chart of Coercion*, http://www.ncdsv.org/images/Chart%20of%20Coercion1.pdf. One of the methods of coercion Biderman outlined was the "monopolization of perception." *See id.* This

Consequently, there is a reduction in the amount of information an individual using a platform is exposed to and consumes. Put differently, platforms—private companies—control the gates to information.[182]

Needless to say, controlling the information gates or having algorithmic control gives platforms immense power. P.W. Singer and Emerson Brooking, the authors of the book *Like War*, discuss social media giving rise to a new information "battlespace" and signal the shifting power dynamic and control platform providers wield over users and nations through their algorithms.[183] To highlight this aspect, the authors deduce that "[w]hile social media has become a battlefield for us all, its creators set its rules . . . a tiny number of individuals can instantly turn the tide of an information war one way or another."[184] Professor Siva Vaidhyanathan similarly argues in his book that "Facebook dominates the media ecosystem. Even small changes in Facebook's design or algorithmic emphasis can alter the political fortunes of an entire nation."[185]

method included fixing the attention of the victim on the immediate predicament and eliminating competing stimuli with those controlled by the captor. *Id.* In some cases, social media's algorithms create similar effects by creating echo chambers void of competing information. While an extreme comparison, it highlights the type of psychological impacts from social media platforms directly affecting individuals, which can then be compounded by the effects of information warfare or abusive trolling, for example. It is hard to ignore these virtual forms of assault on platform users today; these compounding effects could be categorized as a form of informational violence on individuals.

[182] In June 2019, Chairman Jerrold Nadler (D-NY) of the House Committee on the Judiciary recognized this current situation and stated: "there is growing evidence that a handful of gatekeepers have come to capture control over key arteries of online commerce, content, and communications." H.R. Comm. on Judiciary, *Digit. Mkt. Investigation*, H. JUDICIARY COMM. (last accessed May 14, 2020), https://judiciary.house.gov/issues/issue/?IssueID=14921.

[183] *See* SINGER & BROOKING, *supra* note 42, at 21; *see also* Jayamaha & Matisek, *supra* note 55, at 11.

[184] SINGER & BROOKING, *supra* note 42, at 21.

[185] VAIDHYANATHAN, *supra* note 20, at 194.

Microtargeting, algorithmic control, and self-admitted manipulative "information laboratories"[186] created by platforms, therefore, point in the opposite direction of Justice Brennan's vision of "uninhibited, robust, and wide-open" forums for public debate.[187] Such a notion is practically antithetical to the business and algorithmic models of most social media platforms today. In sum, the practical effects of social media platforms serving as the marketplace of ideas generally results in less exposure and consumption of information. In other words, it results in less "competition of the market."[188] Private platforms effectively replaced the government as the main threat to the marketplace, flipping Holmes' marketplace on its head.[189]

On the other hand, there is still an argument that social media merely adds to distributed discovery, which allows users to be exposed to a wider diversity of views, especially in the context of news reports.[190] However, even research suggesting this positive impact also notes there is an overall decline of trust in the news since the rise of social media.[191] Today, approximately sixty-four percent of Americans question whether their news is real or fake.[192] This is because social media gives individuals the "ability to post information to many

[186] Cohen, *supra* note 102, at 165.
[187] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).
[188] Vincent Blasi, *Holmes and the Marketplace of Ideas*, 2004 SUP. CT. REV. 1, 24 (2004).
[189] *See* Wu, *supra* note 173, at 554 (arguing that all of the underlying assumptions that guided the original development of the First Amendment are now obsolete due to the rise in importance of attention markets and changes in communications technologies).
[190] Brennen, *supra* note 25.
[191] *See id.*
[192] *Id.* The overall surge in "fake news" or disinformation and misinformation made possible by social media platforms has led to what RAND researchers call a "truth decay." Mike Ananny, *The Partnership Press: Lessons for Platform-Publisher Collaborations as Facebook and News Outlets Team to Fight Misinformation*, COLUM. JOURNALISM REV. 8 (Apr. 2018), https://www.cjr.org/tow_center_reports/partnership-press-facebook-news-outlets-team-fight-misinformation.php.

people, at any time and with limited regulation."[193] Those traditional gatekeepers of truthful or factual information are no longer in the picture.[194] Coupling these studies with the confinement or targeting of information by platforms frays the conception that the social media speech market serves as a traditional marketplace of ideas, elucidating the truth and promoting individual autonomy or self-government.[195]

After identifying a breakdown in our conventional conception of the marketplace of ideas when juxtaposed against social media platforms, we have to reevaluate Holmes' marketplace more generally. As an initial matter, we must ask ourselves whether the marketplace of ideas can still serve as a conceptual cornerstone of the First Amendment in today's information environment. The simple answer is yes, but this involves revisiting all the basic values of the First Amendment and applying them to the challenges of our new marketplace to determine whether regulation is appropriate.

Those basic values of the First Amendment, neatly categorized by Professor Vincent Blasi, that might be served by a robust free speech principle include (1) individual autonomy; (2) truth seeking; (3) self-government; (4) checking abuses of power; and (5) the promotion of good character.[196] Professor Blasi further asserts that free speech might serve these values by functioning as: (1) a privileged activity; (2) a social mechanism; or (3) a cultural force.[197] Holmes' foundational metaphor of the marketplace instead developed to focus attention primarily on those values of "truth seeking and self-

[193] Marc Trotochaud & Matthew Watson, *Misinformation and Disinformation: An Increasingly Apparent Threat to Global Health Security,* THE BIFURCATED NEEDLE: JOHNS HOPKINS CTR. FOR HEALTH SECURITY (Nov. 29, 2018), http://www.bifurcatedneedle.com/new-blog/2018/11/29/misinformation-and-disinformation-an-increasingly-apparent-threat-to-global-health-security.

[194] *Id.*

[195] The entire data collection model of platforms that drives the current speech market of social media platforms challenges at the core our very notion of individual information self-determination. *See* Khan & Pozen, *supra* note 175, at 512. *See generally* Alessandro Mantelero & Giuseppe Vaciago, *Data Protection in a Big Data Society. Ideas for a Future Regulation*, 15 Digital Investigation 104-109 (2015).

[196] Blasi, *supra* note 188, at 1.

[197] *Id.*

government" served by a free speech principle and "on the function of free speech as a social mechanism."[198] Over time, the other values outlined by Professor Blasi disappeared in the background and rarely informed the conventional perception of the First Amendment. Accordingly, as platforms rapidly become the new marketplace for human activity and social media takes its place as the new public square and social mechanism of choice,[199] individuals and government perceive it near impossible to regulate this space within existing legal and regulatory structures.[200]

Professor Blasi provides a starting place to help us rebuild our notion of the marketplace. He argues that the concept of the marketplace of ideas has more to do with checking abuses of power, the promotion of good character, and serving as a cultural force "than with the implausible vision of a self-correcting, knowledge-maximizing, judgment-optimizing, consent-generating, and participation enabling social mechanism."[201] Therefore, we should at least start by reconceptualizing these critical, yet overlooked, values if we want to maintain our marketplace metaphor for understanding the First Amendment.

To visualize how this might work for all values, and most important in the context of information platforms, we can start to

---

[198] *Id.*; *cf.* Cohen, *supra* note 102, at 161 (describing the current understanding of the marketplace as "an arena for neutral truth production through deliberate, reasoned exchange, where the goods on offer can be evaluated on their merits, where the volume and quality of information are regulated by the laws of supply and demand").

[199] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017). *But see Packingham*, 137 S. Ct. at 1738 (Alito, J., concurring) (disagreeing with equating the entirety of the internet with public streets and parks); Goldenziel & Cheema, *supra* note 5, at 101 (arguing that the metaphor of a public square for social media fails to recognize its implications, specifically, that social media is only one part of the Internet and wholly distinct from the idealized public square assumed in free speech jurisprudence).

[200] *See, e.g.*, Tom Wheeler, *A Focused Federal Agency is Necessary to Oversee Big Tech*, BROOKINGS (Feb. 10, 2021), https://www.brookings.edu/research/a-focused-federal-agency-is-necessary-to-oversee-big-tech/.

[201] Blasi, *supra* note 188, at 2.

reconceptualize a check on the abuses of power. Professor Blasi argues that one of the problems with emphasizing a conventional ideal of a well-functioning market in ideas, without fully understanding all the values free speech serves, is that it produces "dangerous regulatory proposals that attempt to redistribute communicative power."[202] He notes that when Holmes spoke of checks on abuse of power, he often referred generally to the "dominant power" or force in the community in his works—not necessarily government power.[203] Consequently, Holmes' conception of power had more to do with a general sense of power than a political one. In that case, we should implement regulations that manage and recalibrate communicative power more generally, placing checks on the dominant power—information platforms, for example—while still preserving their rights.

The notion that free speech rights protect against the dominant power more generally is also supported by looking at how the freedom of speech has historically been protected. Studying those protections, though, may require examination beyond the Supreme Court's First Amendment cases.[204] Professor Genevieve Lakier argues this notion by showing a different conception of the freedom of speech that the Supreme Court has failed to animate but has nonetheless been embraced in state and federal laws, regulatory policies, and state court decisions.[205] She argues that this body of free speech law explicitly articulates a different viewpoint and supporting principles behind the freedom of speech than that in the Court's First Amendment cases.[206] Specifically, Professor Lakier shows that this body of free speech law provides legal protections for speech and association that are "much

[202] *Id.* Interestingly, Professor Blasi's warning that a failure to reconceptualize the values of the First Amendment would result in dangerous regulatory proposals that redistribute communicative power came just before the explosion of the social media platform and its firm establishment in the American way of life. Now, more than ever, his warnings ring true.

[203] Blasi, *supra* note 188, at 4-5 (citing Holmes, Montesquieu, in *Law and the Court*, in Collected Legal Papers at 250, 258 (1930)).

[204] *See generally* Genevieve Lakier, *The Non-First Amendment Law of Speech*, 134 HARV. L. REV. 2299, 2304 (2021).

[205] *E.g.*, *id.* at 2304-05.

[206] *See id.*

more concerned with the threat that private economic power poses to expressive freedom, and much less *laissez-faire* in its understanding of the government's responsibilities vis a vis the marketplace of ideas."[207]

Better understanding and coming to terms with these powerful animating ideals and historical notions of the freedom of speech and the First Amendment is a significant step toward embracing some of these important values when conceptualizing the First Amendment and the free speech doctrine. It is this type of examination and questioning that is required for us to better understand or rebuild our conception of a functioning marketplace in the context of the new speech market.

3. Reconsidering Regulation: A Government Duty to Protect the First Amendment?

Next, there is a question about the scope of government duties. Even if one reconceptualizes the marketplace of ideas, what role does government play in rebuilding this marketplace held in private hands? Does the creation of marketplace failure by social media platforms mean that government must step in to correct that failure? Or, must society just deal with the consequences and accept the complete privatization of public rights?

Typically, the answer to this question is often premised on a discussion of negative rights, in that the government has no affirmative duty to effectuate those rights within the Bill of Rights. Many constitutional scholars argue that people only have the negative right of non-interference by the government in the realm of the First Amendment or other rights elucidated in the Bill of Rights.[208]

---

[207] *See id.* at 2304.

[208] *See, e.g.*, LAWRENCE TRIBE, AMERICAN CONSTITUTIONAL LAW § 7-2, at 551-53 (2d ed. 1988) (discussing the Fourteenth Amendment Privileges and Immunities historical and early interpretations in terms of negative rights). Professor Michael J. Gerhardt notes that the distinction between negative and positive rights received its classical development through a series of scholarship between the late 1960s and 1980s. *See* Michael J. Gerhardt, *The Ripple Effect of Slaughter-House: A Critique of a Negative Rights View of the Constitution*, 43 VAND. L. REV. 409, nn.6-7 (1990).

However, that analysis overlooks a more nuanced discussion about the distinction and interconnected nature of the Constitution and Bill of Rights themselves; or more broadly, it misses the discussion on the "first duty" of government to protect its citizens' life and liberty.[209]

While the scope of that discussion evades this article, it is enough to address that government may have an affirmative duty to protect the ideals of the First Amendment—that the First Amendment creates not just rights but certain duties.[210] Professor Wu makes a convincing argument on this point. He asserts that American constitutional law says that the First Amendment creates not just rights but certain duties of the government, such as the duty to protect speakers and channels of expression.[211] Professor Wu concludes that we need to recognize the duty of those who enforce the laws to uphold the First Amendment by defending principal channels of online speech, including the protection of "speakers from private efforts to silence them."[212] If those who enforce the laws, specifically the executive branch or law enforcement, have a duty to enforce the laws

[209] *See* U.S. CONST. art. I, § 8 (specifying that Congress, for example, shall provide for the common defense and general welfare and repel invasions); U.S. CONST. amend. XIV (specifying that no State may deprive persons of life without due process of law); *cf.* Steven J. Heyman, *The First Duty of Government: Protection, Liberty and the Fourteenth Amendment*, 41 DUKE L. J. 507 (1991) (arguing that the Constitution requires government to protect from private harms); Gerhardt, *supra* note 208, at 410-413 (critiquing the negative rights view of the Constitution and alternatively arguing for a view of the Constitution in terms of positive rights that impose affirmative duties on the government to meet the needs of certain citizens). Arguably, the government has more of a legal obligation to protect its citizens when the actor is a state-sponsored foreign adversary, as would be the case here, rather than just a private actor. *See also* International Covenant on Civil and Political Rights, adopted Dec. 19, 1966, 999 U.N.T.S. 171, art. 6 (entered into force Mar. 23, 1976). The United States ratified the treaty Sept. 8, 1992. A 2018 Human Rights Council U.N. General Assembly Resolution was adopted affirming that the same human rights that people have offline must be protected online. *See* Human Rights Council Res. 38/7, U.N. Doc. A/HRC/RES/38/7 (July 17, 2018).

[210] Wu, *supra* note 173, at 550. In an information age, channels of expression, information or data are critical infrastructure. By regulating these channels of expression, the government can protect speakers from being silenced in this new public square. *See* Graham, *supra* note 168.

[211] *Id.*

[212] Wu, *supra* note 173, at 550, 572.

to protect channels of online speech, then it must follow that the legislature has a similar duty to make such laws to those ends. Accordingly, government regulation of social media platforms in the form of overseeing business practices and algorithms may be necessary.

Regulation would not, of course, be necessary for the censorship of speech or information. Instead, regulation may be seen as a requirement for government to fulfill its duty of ensuring that the "most important place for the exchange of views"[213] remains open, that speakers and channels of expression are protected, and that the speech market functions as it was envisioned to operate—even while maintained in private hands. Government, therefore, is not censoring speech through regulation; it is protecting the channels of speech from harmful activity like information warfare campaigns. Additionally, government regulation of platforms can be perceived as necessary to ensure there is not a "balkanization of information consumption,"[214] there is no unlawful hampering of the right to receive foreign or other speech in the first place, and that citizens have the right to have individual thought in today's speech marketplace.

4. First Steps Toward Regulation: Examining Algorithmic Control

If the U.S. government should or must regulate, what might that regulation look like? As argued above, Holmes' marketplace conception leaves the door open to a much broader view of free speech; it is not to be interpreted as qualifying the First Amendment as an absolute right that completely ties the hands of the government for lawmaking and regulation. There are still meaningful limits on the First Amendment where the government may be able to regulate, especially in the context of the right to receive speech. In particular, the government need not turn a blind eye to the rights of listeners and the divisive effects of algorithmic control and amplification on social media. Disclosing sources or marking posts may be one way to combat

[213] Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017).
[214] Goldsmith, *supra* note 14.

this problem.[215] Various scholars have offered, for example, that government may be able to regulate speaker identification in certain situations by requiring platforms to disclose sources or mark certain information for users, especially in the context of spreading political messages.[216] While this sounds like a reasonably feasible solution, users' gravitation toward closed applications or platforms makes this an increasingly ineffective solution.

In a recent article, Professor Joan Donovan and Danah Boyd offered another alternative to looking at this problem by unearthing a 1932 Supreme Court case, *Packer Corp. v. Utah.*[217] *Packer Corp.* involved a company that was prosecuted under a Utah statute, which made it a misdemeanor to display an advertisement for tobacco products in public places but permitted advertisements in periodicals.[218] The case was decided upon Commerce clause and Fourteenth Amendment equal protection grounds; First Amendment issues were not raised by the parties or the Court.[219] Upon these limited legal bases, the Court held the statute's prohibitions were permissible since it addressed only a subset of intrastate advertising based on reasonable grounds for its classification and distinction among other types of advertisements.[220]

Although not decided on First Amendment grounds, Justice Brandeis applied what has become known as the "captive audience" principle to distinguish when the government could regulate advertisements published in a public forum.[221] Specifically, Justice Brandeis argued that the government could place restrictions on

---

[215] Although, users moving more toward the use of closed applications may make this an obsolete solution, or at least not very effective. *See infra* notes 329-31.
[216] *See, e.g.*, BODINE-BARON ET AL., COUNTERING RUSSIAN SOCIAL MEDIA INFLUENCE (2018); *cf.* VAIDHYANATHAN, *supra* note 20, at 197.
[217] Joan Donovan & Danah Boyd, *"Stop the Presses? Moving From Strategic Silence to Strategic Amplification in a Networked Media Ecosystem",* AM. BEHAV. SCIENTIST (Sept. 29, 2019).
[218] Packer Corp. v. Utah, 285 U.S. 105, 107 (1932).
[219] *See generally id.*
[220] *See id.* at 109-11.
[221] *See id.* at 110*; see, e.g.*, Gambino v. Fairfax Cty. Sch. Bd., 429 F. Supp. 731, 735 (E.D. Va. 1977).

billboard advertisements because, unlike magazines, billboards had captive audiences when they were placed on public streets; therefore, billboards were unavoidable to anyone passing through these public forums.[222] The Court focused upon the lack of free choice in viewing advertisements in a public forum located in the state to establish a threshold for appropriate government regulation.[223]

Donovan and Boyd point to this "captive audience" reasoning as a rationale for protecting the rights of listeners. In their summation of *Packer Corp.*, Donovan and Boyd reiterate that "people could choose to look at a magazine, but to avoid a billboard, they'd have to intentionally divert their eyes."[224] They argue this case could stand for the proposition today that speech rights are not curtailed when speakers are denied access to tools of amplification like the billboard, especially if such amplification would be to the detriment of the rights of the listeners.[225] In today's application, such amplification tools might be classified as technologies like bot-nets or underlying platform algorithms, to name the most prominent.

The developing doctrine of listener rights makes this an even more plausible argument today. In particular, a key aspect of listener rights focuses on advancing listeners' First Amendment information-seeking and autonomy-exercising interests.[226] Notably, these are values tied to the foundational animating ideals of the First Amendment that Professor Blasi summarized and are often overlooked in the current functioning of the marketplace of ideas, especially individual autonomy. By refocusing on these core values, we can better navigate through the changing nature of the speech market and rebalance the power of speaker and listener rights.

---

[222] *Packer Corp.*, 285 U.S. at 110.
[223] *Id.*
[224] Donovan & Boyd, *supra* note 217.
[225] *Id.*
[226] *See* RonNell Andersen Jones, *Press Speakers and the First Amendment Rights of Listeners*, 90 U. COLO. L. REV. 499, 500 (2019).

Although speech in public places typically occupies a special position in terms of First Amendment protection,[227] certain types of amplified speech on platforms, such as targeted advertisements, would likely not meet that classification and be afforded such increased protections. Targeted advertisements, in particular, are arguably a clear form of private speech—curtailed and curated for the individual based on algorithmic surveillance; it is specifically not made for greater public consumption. That said, "even protected speech is not equally permissible in all places and at all times."[228] Legislatures may place reasonable time, place, and manner restrictions on certain types of speech.[229] In today's marketplace, such reasonable restrictions may assist in supporting another value of the First Amendment—checking abuses of power. Those abuses can exist between the platforms, the speaker, as well as the listener.

With these considerations in mind, Donovan and Boyd's argument can go a step further. For instance, if *Packer Corp.* is considered in the context of platforms and their sticking power, their control on listeners, and their position as the most important public forum, then it is easy to envision how a social media user might resemble the 1932 "captive audience" driving down the "public street" (then considered the quintessential public forum of its day). As Donovan and Boyd rightly point out, Justice Brandeis observed that billboards on public streets are "constantly before the eyes of observers on the streets and in street cars to be seen without the exercise of choice or volition on their part."[230] In comparison, social media advertisements induce the same required observation without much "exercise of choice or volition" on the user's part.[231] Certainty, social media users' "consent" to use a particular platform,[232] but do they really have a choice on what they see, especially advertisements? Additionally, how can a person navigate and use this new "most

[227] *See* Snyder v. Phelps, 562 U.S. 443, 452, 458 (2011).
[228] *Id.* at 456 (citing Frisby v. Schultz, 487 U.S. 474, 479 (1988)).
[229] *See id.*
[230] Packer Corp. v. Utah, 285 U.S. 105, 110 (1932).
[231] *Id.*
[232] *But see* Zuboff, *supra* note 97, at 233-42 (discussing platforms' use of "terms of sur-render" and that users do not really have a fully informed or consensual choice).

important" public forum without being inundated with advertisements or "curated content"? The answer to this question for the majority of Americans is they cannot.[233] It is constantly before their eyes.

Brandeis went on in *Packer Corp.* to distinguish magazines from billboards by saying that with magazines, "there must be some *seeking* by the one who is to see and read the advertisement."[234] While one can argue this point alone might give social media platforms a pass under *Packer Corp.,* since a user must initially sign up and seek out the use of a platform, it utterly misses today's importance and nature of social media platforms—and other dominant platforms—and the interwoven aspect of platforms into the functioning of our daily lives. Although users "subscribe" to the information platforms, it is how people enter today's public roadway or forum. It just so happens that those public forums are now in private control and require some waiver of our rights—a waiver that is questionable in the first place as to whether users are fully informed or have a true consensual choice before entering. Much of society has had to organize their daily lives, willingly or not, around this fact.

The *Packer Corp.* precedent, therefore, tends to support far more governmental regulation of platforms under a First Amendment conception than currently assumed permissible. Specifically, the *Parker Corp.* precedent supports regulating the underlying algorithms that afford tools like amplification. Regulating methods of amplification used by and within platforms may be more critical with time. A recent study of data manipulation and exploitation on social media platforms suggests that it is getting harder and harder to spot inauthentic content online and there is a growing army of learned manipulators of social media.[235] Thus, as long as the amplification system continues, this army will continue to grow and learn to game the system.[236] Hence, regulation may be the only viable option to

[233] *See infra* notes 321-23.
[234] *Packer Corp.*, 285 U.S. at 110 (emphasis added).
[235] Packer Corp. v. Utah, 285 U.S. 105, 110 (1932).
[236] *Id.*

counter the growth of information harms spurred by algorithmic control and amplification tactics in the new speech market.

B. Reexamining the Bounds of Targeting Foreign Speech

Government regulation of information platforms is not the only avenue of approach for countering information warfare. The direct targeting of malicious foreign speech that constitutes a covert information warfare campaign requires closer examination as well. Americans should not be so quickly deterred by what might seem like an impenetrable First Amendment cloak of protection for the right to receive foreign speech. It too has its limits.

Supreme Court precedents increasingly give "substance and scope to a First Amendment right to receive information and ideas."[237] The Supreme Court in *Stanley v. Georgia*, building on prior Court precedent, established that the freedom of speech and press "necessarily protects the right to receive,"[238] and that this right to receive information and ideas is "fundamental to our free society."[239] Subsequently, Americans have come to accept the general notion that the government may not unduly burden an individual's receipt of information. As many scholars argue, this right includes the right to receive foreign speech. Professor Joseph Thai, for example, reasons that the precedent in *Citizens United v. FEC*, confirms that when the government restricts where a person may get his or her information or what distrusted source he or she may not hear, then it violates the First Amendment protection to think for ourselves.[240] Such

[237] Joseph Thai, *The Right to Receive Foreign Speech*, 71 OKLA. L. REV. 269, 274 (2018).
[238] Stanley v. Georgia, 394 U.S. 557, 564 (1969) (quoting Martin v. City of Struthers, 319 U.S. 141, 143 (1943)).
[239] *Id.*; *see also* Lamont v. Postmaster General, 381 U.S. 301, 306-07 (1965) (holding that Congress, through promulgation of a statute, preventing the U.S. Postal Service from delivering "communist propaganda" pamphlets absent a specific written consent from the addressees violated the First Amendment, as a form of political speech, because it unduly burdened the addressees' right to receive information).
[240] *See* Thai, *supra* note 237, at 294-99 (discussing the sweeping implications of Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010), for First Amendment doctrine right to receive information).

protections, therefore, should make no regard for speaker identification or the fact that the information comes from a foreign country.[241]

One Supreme Court case, recently revisited by the Court, offers insight on some significant bounds for this right to receive information. *Kleindienst v. Mandel*, a 1972 immigration and First Amendment case, presents a pathway for understanding the scope of permissible action by the U.S. government in countering foreign malicious information warfare campaigns that may pass First Amendment scrutiny.

1. *Mandel's* Deferential Review and Military Operations

In *Kleindienst v. Mandel*, the U.S. Attorney General denied Belgian "revolutionary Marxist" journalist, Ernest Mandel, who was invited to speak at a Stanford University conference, admission to the United States.[242] The Attorney General denied entry under the Immigration and Nationality Act (INA) of 1952 that provided certain aliens shall be ineligible to receive visas and are excluded from admission unless a waiver is granted by the Attorney General.[243] Although Mandel had previously been granted waivers for admission to the United States, Mandel's attempt to gain a waiver for travel to attend the Stanford University conference was denied based on prior violations of waiver terms, albeit unknown to Mandel at the time.[244] The University professors challenged Mandel's denial of entry and the constitutionally of the INA based on a claim that their constitutional "right to receive information" was implicated.[245]

Attempting to dispose of the First Amendment claim, the Government initially argued that only action was being regulated through the INA, not speech. In other words, the Government argued there was no restriction on First Amendment rights because what was

[241] *See id.* at 298.
[242] Kleindienst v. Mandel, 408 U.S. 753, 756-57 (1972).
[243] *Id.*
[244] *See id.* at 757-60.
[245] *Id.* at 760.

restricted was "only action—the action of the alien coming into this country."[246] The Government also argued that other forums for Mandel's speech were still available to him even if he was precluded from speaking within the United States.[247] The Court, however, did not find these arguments persuasive, or at least not dispositive. The Court relied on its previous holding in *Lamont v. Postmaster General* to show that regulation bearing directly on physical movement, such as the physical entry of mail into the country, cannot fully answer the mail on First Amendment claims.[248] The Court then pointed out that asserting alternative means of access to Mandel's ideas is merely a relevant factor in balancing First Amendment rights against government regulation, but it does not preclude inquiry into First Amendment implications.[249]

Ultimately ruling against the professors, the Court determined in a limited review, that it was dispositive that the Executive gave a "facially legitimate and bona fide" reason for its action.[250] The Court applied this extremely deferential review to the First Amendment claim even after it reiterated that the First Amendment right to free speech includes a right to receive information.[251] The Court's reasoning for applying the deferential standard mainly rested on the authority of the political branches over the power to exclude aliens, a power "inherent in sovereignty . . . necessary for maintaining normal international relations and defending the country against foreign encroachments and dangers."[252] The Court established and upheld Congress' plenary power to regulate "admission of aliens and to exclude those who possess those characteristics which Congress has forbidden,"[253] and the lawful

[246] *Id.* at 764.
[247] *Id.* at 765.
[248] *Mandel*, 408 U.S. at 765.
[249] *Id.*
[250] *Id.* at 770.
[251] *See id.* at 762-70.
[252] *Id.* at 765.
[253] *Id.* at 766.

delegation to conditionally exercise that power to the Executive.[254] Thus, the Court held

> [W]hen the Executive exercises this power negatively on the basis of a facially legitimate and bona fide reason, the courts will neither look behind the exercise of that discretion, nor test it by balancing its justification against the First Amendment interests of those who seek personal communication with the applicant.[255]

Recently, the Court reaffirmed and applied this deferential standard in *Trump v. Hawaii*. In this 2018 case, the Supreme Court reviewed its line of cases where *Mandel's* deferential standard of review was applied in similar contexts and constitutional claims. In *Trump*, the Court again applied this deferential standard to a First Amendment Establishment Clause claim. Reiterating respect for the political branches' broad power over the creation and administration of the immigration system, the Court determined the government need only provide a statutory citation to explain a visa denial.[256] Moreover, the Court in *Trump* emphasized that *Mandel's* narrow standard of review "has particular force" in such cases that intersect "the area of national security."[257] The Court noted that judicial inquiry into the national-security realm raises concerns for the separation of powers by intruding on the President's constitutional responsibilities in the area of foreign affairs.[258]

Mandel and cases following its reasoning, like *Trump,* are key to understanding that the right to receive foreign speech is not all-encompassing and has some significant boundaries. The reasoning applied in *Mandel* and *Trump* by the Court elucidates how the exercise of Congress' plenary power, coupled with congressionally supported and constitutional Executive action, can overcome the First Amendment right to receive claims with a narrow standard of review.

---

[254] *Mandel*, 408 U.S. at 770.
[255] *Id.*
[256] *See* Trump v. Hawaii, 138 S. Ct. 2392, 2419-20 (2018).
[257] *Id.* at 2419.
[258] *Id.*

As an analogy, the political branches' broad power over foreign military action in the interests of national security should similarly receive such a deferential standard of review. Thus, congressionally authorized military action, coupled with the President's carrying out of his Constitutional responsibilities for foreign affairs and as Commander-in-Chief, offer significant and clear authorities for countering malicious foreign speech abroad. In other words, the Supreme Court would likely uphold any congressionally authorized military operation taken outside the United States pursuant to authorized Executive action to target and disrupt adversarial information warfare campaigns by a foreign state entity or agent. This might include, for instance, disrupting an adversarial state-sponsored propaganda-making information platform or disrupting that state actor's access to foreign or domestic platforms—all of which could tangentially implicate U.S. citizens' right to receive that foreign speech.

When analyzing this hypothetical scenario, we must first keep in mind the Court's caution from *Mandel* that we cannot foreclose a First Amendment right to receive claim based on assertions that shutting down such covert information warfare operations is merely restricting the action of the operation,[259] or that targeting one platform may still leave alternative forums open. *Mandel* indicates these are not dispositive arguments but are rather mere factors for consideration. The crux of the analysis, though, rests on whether there is an exercise of plenary power by Congress to regulate and a lawful authority for Executive action, creating the political branches' broad power to trigger *Mandel's* deferential or narrow standard of review. In the case

[259] *But cf.* Sujit Raman, *The Rule of Law in the Age of Great Power Competition in Cyberspace,* DOJ (May 21, 2019), https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-aba-rule-law-initiative (discussing the use of government affirmative action to prevent "covert, cyber-enabled foreign influence campaigns that are designed to attack and undermine our elections through the weaponization of speech" without any implication of the First Amendment because the First Amendment does not protect a right to receive "covert foreign propaganda").

of authorized military action for national security purposes, this is easy to foresee.

The U.S. Constitution provides Congress and the Executive broad authorities to defend the nation.[260] There is certainly a long history of these political branches using this authority to defend against foreign interference. Congress also recently provided explicit positive authority to the Executive in Section 1642(a) of the National Defense Authorization Act (NDAA) for the fiscal year 2019, which provides the Executive authority to "disrupt, defeat, and deter cyber attacks" against Russia, China, North Korea, and Iran in cyberspace, "including attempting to influence American elections and democratic political processes."[261] As the joint explanatory statement shows, Congress provided this authorization to counter "Russia's information operations against the United States and European allies in an attempt to undermine democracy."[262] Military action that targets foreign information warfare campaigns by those named States, therefore, is supported by the plenary power of Congress to wage war and raise armies and the Executives' power to conduct foreign affairs and serve as Commander-in-Chief.

Presuming then, that there is supporting intelligence for an ongoing influence campaign that fits into the context of section 1642's authority, a First Amendment claim asserting that the disruption of such information from coming into the United States infringes on the right to receive foreign speech would be unlikely to prevail. *Mandel's* deferential standard of review would apply to such claims since the political branches exercised lawful authority "on the basis of a facially legitimate and bona fide reason."[263] The Court would look no further

[260] U.S. CONST. art. I, § 8, cl. 1.1; U.S. CONST. art. II, § 2, cl. 1-2.
[261] Pub. L. No. 115–232, div. A, tit. XVI, §1642(a)(1) (2018).
[262] *Joint Explanatory Statement of the Committee of Conference to Accompany H.R. 5515* (2019) (statement on Section 1642(a) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, H. Rept. 115-874)[hereinafter *Explanatory Statement*], available at https://rules.house.gov/sites/democrats.rules.house.gov/files/JointExplanatory%20Statement.pdf.
[263] Kleindienst v. Mandel, 408 U.S. 753, 770 (1972).

behind the reasons offered by the Executive or weigh the First Amendment rights of those individuals burdened by the action. The fact that the issue implicates national security concerns only further weighs in favor of the Government.

2. Circumventing the First Amendment Altogether?

While the analysis above does not necessarily circumvent the First Amendment, there is one consideration for government action that may avoid First Amendment implications altogether. Section 1642(b) of the fiscal year 2019 NDAA provides the Secretary of Defense with the authority to make arrangements with private sector entities, on a voluntary basis, to share threat information related to malicious cyber actors and any associated false online personas, as associated with section 1642(a).[264] For this provision, Congress explicitly considered the government, DoD in this case, as notifying social media companies for terms of service violations by any of its users that qualified under the limits of 1642(a) so that the social media companies could take action.[265] Action would likely include exclusion from the social media platform, like most terms of service provisions provide. So essentially, Congress gave DoD authority to assist in removing a specific subset of foreign speech from the speech market. While it might sound suspect, it does not appear to implicate the First Amendment, generally.

Although Congress explicitly authorized the Executive to take this type of action within the limits of section 1642(a), this type of congressional authorization is likely not even required for such action. Critically, it highlights another way government can influence foreign speech without implicating the First Amendment: to go through the true power brokers of speech—the information platforms themselves. Because of platforms' immense power to control and moderate speech today, the new public forum may not have as many real First Amendment considerations at all. The government would be generally protected from any state action doctrine that might be asserted when

[264] *See* Pub. L. No. 115–232, div. A, title XVI, §1642(b) (2018).
[265] *Explanatory Statement*, *supra* note 262 (statement on Section 1642(b)).

providing information about terms of service violations because of the platforms' sole power to do as it pleases on its own platform.

In fact, U.S. laws created this imbalance of power. Section 230 of the CDA gives these platforms even more immunity and discretion to do as they please on their platforms and make and act on their terms of service as they see fit. Effectively, the government now has its own shield against First Amendment claims when it provides information about speech it disagrees with to social media platforms, albeit the final arbiter is the platform. Perhaps then, the only influence on those platforms is the speech norms that crop up around the platform and keep its bottom-line profits rising.

C. Another Look at Harm: Addressing Falsehoods and Fake News

One final aspect of content that needs revisiting based on its prevalence in today's discourse within the new speech market is falsehoods. The jurisprudence on falsehoods can likely do more work to fill the gaps for reshaping how Americans view First Amendment limits on addressing information harms like "fake news," "propaganda," or "disinformation."[266] A plurality in *United States v. Alvarez* affirmed that falsehoods are protected speech, but acknowledged that certain finely tailored exceptions exist for government to regulate false information that causes a "legally cognizable harm," such as fraud or defamation.[267] Professor Thai cautions, however, that such harms still have to be finely tailored to take into account both government interests and harms that the market cannot correct.[268]

One case for regulating a legally cognizable harm that the market cannot correct and could be finely tailored to further a

[266] Generally speaking, all of these terms have the same result: "a constant and alarming undermining of public trust in expertise and the possibility of rational deliberation and debate." VAIDHYANATHAN, *supra* note 20, at 11.
[267] *See* United States v. Alvarez, 567 U.S. 709, 719 (2012).
[268] Joseph Thai, Comments, USCYBERCOM Legal Conference (Mar. 3, 2020); *see also* Thai, *supra* note 237, at 303-04.

legitimate government interest of global health security are threats to public health through disinformation, as discussed in Part II.C. This seems particularly apt in today's environment of a global pandemic. Disinformation about public health advice during a pandemic—likely to lead to physical civilian harm—instinctually feels like it should qualify as a legally cognizable harm if the Supreme Court views fraud, defamation, and perjury as qualifying "legally cognizable harms."

But, disinformation about public health does not facially appear like the type of "concrete" legally cognizable injury the Supreme Court envisioned.[269] However, as discussed in Part II.C, evidence has been mounting over the years to show the effects of social media platforms on the digestion of information and the direct foreseeable link between disinformation and civilian harm, most especially in the context of public health.[270] Furthermore, in *Alvarez*, Justice Breyer, concurring in the judgment with Justice Kagan, advocated for an approach that asks "whether the statute works speech-related harm that is out of proportion to its justifications."[271] Although this approach was not echoed throughout the plurality opinion, one might look to it as a jumping-off point for future legal and policy arguments about where the First Amendment jurisprudence should be headed in guiding future laws concerning this type of disinformation. Health disinformation, like an anti-vaccination campaign, that could cause an entire population to fail to achieve herd immunity seems like it should pass the test. The speech-related harm would be well out of proportion to its justifications if it meant causing fatalities for a significant portion of the population. Such harms might even be envisioned as reaching the level of constituting a type of individual informational violence.[272] A legally

[269] *See id.* at, 302-05.

[270] *See infra* Part II.C, notes 129-32, 145-47.

[271] *See* Thai, *supra* note 237, at 303 (citing United States v. Alvarez, 567 U.S. 709, 730 (2012)).

[272] *See* discussion *supra* note 195. Government has a duty to protect individuals against violence, and this could be reinterpreted today in a domestic context as individual informational "private violence," especially if cyberspace is where we now conduct our daily lives as well as wage our wars. *See* Heyman, *supra* note 209, at 510,

cognizable harm could also be considered in terms of informational violence to a nation state,[273] in that, a widespread foreign influence campaign—including disinformation on all topics from politics to public health—may violate state sovereignty under international law.[274] A violation of a state's sovereignty would be viewed as another legally cognizable harm recognized domestically and internationally.[275]

This level of recognition for informational violence is admittedly still in its infancy.[276] These concepts have yet to take hold in any large-scale international, domestic internal government, or academic discussions.[277] This fringe opinion might get more traction when society starts to see the real costs of information warfare campaigns that cause direct harm to civilians. That empirical evidence is likely closer than we think as we live through this pandemic and start to see information harms crop up all around us that attempt to exploit this issue.

Nevertheless, it is certainly enough to know that the government's hands are not completely tied when it comes to regulating this new market and public square held in private control. As Professor Wu rightly states, "the legal system need not sit on the sidelines" to protect a healthy speech environment.[278] Imperatively, America must first start to re-envision its conception of the marketplace of ideas and the limits on government and what they mean for the protection of the First Amendment. How Americans come to view the speech market today and interpret and develop First

536 ("The paradigmatic instance was the government's duty to protect individuals against violence" and this duty was understood to include the responsibility of government to prevent violence before it occurred.").

[273] *See* HAATAJA, *supra* note 82, 54-62.

[274] *See id.*

[275] *See id.*

[276] Only a small body of academic research has begun to examine this notion. *See generally.*, HAATAJA, *supra* note 82 (drawing on Luciano Floridi's information ethics).

[277] *Cf. supra* notes 143-45.

[278] Wu, *supra* note 173, at 549-50.

Amendment jurisprudence is critical for recalibrating the balance of the private-public (public, in this instance, meaning civil society) power and control, fixing information harms, and reestablishing the protections and underlying values of the First Amendment.

D. Contemplating Future Regulatory Steps: Social Media as Critical Infrastructure

A reconceptualization of how the First Amendment and the regulatory environment interact with platforms and government moves the United States closer to filling the gaps in its domestic legal framework needed to address information warfare. Another step in changing the framework to better capture the government's duties and balance private rights is to designate social media platforms as critical infrastructure. Understandably, suggesting such a solution to First Amendment or content concerns may seem out of place and raise its own set of concerns with possible government entanglement in speech. Proposing this reform within this context, though, is meant to serve as a key example of how the nation may need to reconceptualize traditional approaches to reforming the law—framing biases often get in the way of reform.

Placing the moniker of critical infrastructure on social media platforms is a good starting place for rethinking reform for multiple reasons. Designating social media as critical infrastructure provides the government a mechanism to meaningfully assist in the clean-up of information harms from the speech environment while staying within the limits of the First Amendment. The infrastructure analogy also aptly fits how platforms serve American interests today. Many already recognize the role that information communication platforms play as a form of infrastructure or public utility.[279] This is nearly undeniable while currently living through a global pandemic that requires social distancing and the use of these speech environments to conduct daily

[279] *See, e.g.*, Khan & Pozen, *supra* note 175, at 508-09. *See generally* Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621 (2018). Even U.S. government leaders suggested designating social media a public utility. *See* SCIUTTO, *supra* note 2, at 261.

life and receive important information. Most notably, categorizing information platforms, social media platforms in particular,[280] as critical infrastructure would subject platforms to light-touch regulatory regimes, government assistance and oversight for critical emergency response, and voluntary cooperation with other critical infrastructure sectors and government.

1. Addressing Dangerous Relationships and Failing Alternatives

A major hurdle for this proposed reform is the concern that the more the U.S. government becomes entangled with the self-regulation of private entities or online platforms, the more the First Amendment is implicated. Specifically, the concern is that a platform's behavior may then be perceived as constituting state action in certain circumstances.[281] This concern controls the government's relationship with information platforms today. Therefore, the government leaves social media companies or other platforms to operate independently and regulate content on their platform to hopefully avoid those assumed First Amendment issues.[282]

However, as discussed above, in today's power dynamic, this is truly less of a concern. Under this prevailing assumption, government and platforms instead created dangerous relationships and corresponding "regulatory proposals that attempt to redistribute communicative power."[283] Further, it is false to believe that government must be completely hands-off when it comes to platform regulation. The government may have a duty to act and the current platform economy may be providing the government a complete run around the First Amendment altogether—thereby hampering the

[280] Arguments can be made that this should also extend to other communication and services platforms, such as Amazon, Google, or Apple, to name a few major platforms.
[281] *See* Goldenziel & Cheema, *supra* note 5, at 156.
[282] *See id.*
[283] Blasi, *supra* note 188, at 2.

realization of its animating values. Entanglement may not necessarily be a bad thing in some cases.

By the government carrying out this false assumption that there must be a regulatory void, social media platforms gained immense power and control over the speech environment and their users.[284] Scholars elucidated how the rapid rise to power of social media platforms allowed them to emerge as governors over their users,[285] or reach a status as some type of sovereign entity that is untouchable by government oversight and regulation.[286] A disproportionate and unprecedented power balance and dangerous relationships between the private sector, the government, and the individual emerged as a result. With private companies governing over the new public square, citizens are left without recourse and the realization of individual rights because they do not have the same negative rights against private companies as they do against the government.[287] This is the speech environment where a private company has the sole control and power to decide when or how to "deplatform" a sitting U.S. President without real judicial scrutiny and foreclose important channels of communication in the modern public square (putting aside whether you agree with the speech or not or whether such action should have been taken sooner rather than later, or even at all).

Platforms are gaining control over the government. As government further embeds itself in this assumption that it must rely on voluntary platform action to solve information harms, the relationship with government and platforms becomes even more tenuous and foreboding. The government finds itself beholden to platforms under the false assumption that their hands are tied to regulate the speech environment.[288] Such a relationship can only work

[284] *See* discussion *supra* Section III.B.1.i.
[285] *See generally* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018) (describing social media platform's regulation of speech as a form of "governance").
[286] *See* Cohen, *supra* note 98, at 199-203.
[287] Goldenziel & Cheema, *supra* note 5, at 100.
[288] *See* Khan & Pozen, *supra* note 175, at 537.

to the platforms' advantage in continuing to advocate and achieve lesser and lesser controls on platforms, thereby increasing their power and position over society in exchange for the government receiving what seems like a quick fix to information harms.

Relying on platforms to solve information harms,[289] though, fails to recognize platforms' status as a primary fiduciary to stakeholders—not the government or American people. A platform's core business model and duties under current law bely removing information harms.[290] Instead, their business model advances placating government only to the extent that keeps them coming back in false reliance on quick fixes so that they may avoid future regulation. This is a dangerous relationship to maintain.

Some scholars offer other solutions to these dangerous relationships, such as enacting laws that would create a fiduciary relationship between platforms and users. Professor Balkin asserts that such a relationship may solve information harms by creating some responsibility on platforms for user protections.[291] But, as Professors Khan and Pozen argue, the concept of a fiduciary relationship with a user is completely incongruous with reality.[292] There is no logical way to carry out such a fiduciary duty given the current tension in the law between a company's fiduciary duties to its stakeholders and proposed duties to its users.[293] A fiduciary relationship, like the one advocated by Professor Balkin, would essentially collapse the underlying business model of the platform if taken to mean the same type of fiduciary duty that exists under the law between lawyer and client or physician and

[289] For instance, this might entail government agencies requesting that certain foreign influence campaign information on social media platforms be removed or marked by the platforms voluntarily.

[290] *See generally* Carrie Cordero, *Corporate Data Collection and U.S. National Security: Expanding The Conversation in an Era of Nation State Cyber Aggression*, LAWFARE (June 1, 2018), https://www.lawfareblog.com/corporate-data-collection-and-us-national-security-expanding-conversation-era-nation-state-cyber; Khan & Pozen, *supra* note 175, at 497.

[291] *See* Khan & Pozen, *supra* note 175, at 499.

[292] *See generally id.*

[293] *See id.* at 502-08.

patient, for instance. Moreover, Professors Khan and Pozen demonstrate why it is dangerous to think of a platform as a fiduciary: such a designation may result in elevating platforms to an almost untouchable level with government and government regulators.[294]

Most concerning, the fiduciary duties advocated by Professor Balkin can easily be manipulated and interpreted in a manner that wholly benefits the platform. There is nothing to stop the proposed platform fiduciary from interpreting what is assumed best for the user, and that might be more targeted advertising and more algorithmic control. Surely, a platform can argue these "information laboratories"[295] work to the advantage of the user and give them the best user experience possible. Who wouldn't want to be persistently surveilled and have their human experience turned into raw material for sale to gain a custom experience? Sarcasm aside, we should immediately raise an eyebrow when Mark Zuckerberg himself, who supports the fiduciary concept, stated in a 2018 interview with Professor Zittran (also a proponent of the fiduciary concept) that the fiduciary relationship could get interesting when deciding who decides what is in a user's best interest.[296]

Based on the concerns above, it would serve the government well to look elsewhere in the law to rectify these relationships. The government needs a solution that does not tie its hands or make it beholden to platforms. Government, rather, needs a legal solution that provides it with the space and freedom of movement to carry out its duties of protecting the speech environment and addressing information harms.

---

[294] *Id.* at 537.

[295] Cohen, *supra* note 98, at 165.

[296] *At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements*, HARV. L. TODAY (Feb. 20, 2019), https://today.law.harvard.edu/at-harvard-law-zittrain-and-zuckerberg-discuss-encryption-information-fiduciaries-and-targeted-advertisements/.

2. Designating Social Media Platforms as Critical Infrastructure

Critical infrastructure is defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the nation's security, economic stability, public health or safety, or any combination of these factors."[297] There are currently sixteen critical infrastructure sectors that "include, among other things, banking and financing institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned and operated by the private sector."[298] Designating a public utility or private entity critical infrastructure acknowledges the vital role those utilities or entities play in carrying out the daily functions of Americans.

In 2017, in response to the 2016 U.S. election interference, the Executive branch designated election infrastructure as part of the critical infrastructure scheme.[299] The U.S. government recognized that the election infrastructure secures a major part of Americans' democratic way of life, and allowing it to be tampered with by foreign adversaries challenges that way of life.[300] The Executive branch should have taken these efforts a step further by designating social media platforms as critical infrastructure. Doing so would have recognized that the real upheaval of democracy and the U.S. election was waged

---

[297] 42 U.S.C. § 5195c(e); GOV'T ACCOUNTABILITY OFF., CRITICAL INFRASTRUCTURE PROTECTION: ADDITIONAL ACTIONS ARE ESSENTIAL FOR ASSESSING CYBERSECURITY 4 (Feb. 2018), https://www.gao.gov/assets/700/690112.pdf; DEP'T HOMELAND SEC., CRITICAL INFRASTRUCTURE SECURITY, (July 14, 2020), https://www.dhs.gov/topic/critical-infrastructure-security (clarifying the definition to describe "*the physical and cyber* systems and assets").

[298] GOV'T ACCOUNTABILITY OFF., *supra* note 297, at 4.

[299] *See* DEP'T OF HOMELAND SEC. OFF. OF THE PRESS SEC., STATEMENT BY SECRETARY JEH JOHNSON ON THE DESIGNATION OF ELECTION INFRASTRUCTURE AS A CRITICAL INFRASTRUCTURE SUBSECTOR (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[300] *See id.*

on those platforms.[301] Put simply, social media platforms have become a vital aspect of the critical infrastructure of our democracy.[302]

A meaningful advantage for designating an entity as critical infrastructure is that the designation carries all the "domestic and international benefits and protections of critical infrastructure that the government has to offer."[303] These "benefits and protections," for example, can serve as a signal to foreign adversaries that these entities are off-limits for attack or interference in peacetime since under international law critical infrastructure should typically be left to the principle of non-interference.[304] Additionally, a critical infrastructure designation allows the government to carry out its duties in an oversight and regulatory structure with boundaries that are clearly defined and transparent to the public for the ultimate protection of citizens' right to life and liberty in a free democracy.[305] The designation does this by triggering the application of various regulations and policies that foster a collaborative relationship with the government, fueled by information sharing and security oversight and assistance.[306]

Security oversight and voluntary cybersecurity frameworks that incorporate government and private sector best practices is a key

---

[301] *See, e.g.*, Goldsmith, *supra* note 14 (The weaponization of social media "called into question the legitimacy of the election and of the democratic system more broadly.").

[302] Stefan Heumann, *Why Social Media Platforms Should be Treated as Critical Infrastructure*, MEDIUM (Oct. 12, 2018), https://medium.com/election-interference-in-the-digital-age/why-social-media-platforms-should-be-treated-as-critical-infrastructures-6a437a127ff7.

[303] DEP'T OF HOMELAND SEC. OFF. OF THE PRESS SEC., *supra* note 299.

[304] Kaveh Waddell, *Why Elections Are Now Classified as 'Critical Infrastructure'*, THE ATLANTIC (Jan. 13, 2017), https://www.theatlantic.com/technology/archive/2017/01/why-the-government-classified-elections-as-critical-infrastructure/513122/.

[305] *See generally* DEP'T OF HOMELAND SEC., PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Dec. 2013).

[306] *See* Heumann, *supra* note 302; *see also* CISA, A GUIDE TO CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, 11-12 (Nov. 2019), https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

feature of the critical infrastructure regime.[307] The government provides guidance, incentives, and requested assistance for the implementation of higher technical security standards that protect user data and physical network infrastructures from outside interference or malicious activities. The primary cause of poor cybersecurity on private systems and networks is inadequate regulation,[308] thus, the modicum of "regulation" provided through the critical infrastructure regime is critical for enhancing the overall security of these entities. Protecting data and networks is highly important for combating information harms. This is especially the case in an information era where access to data means access to people, which is discussed further in Part IV. To achieve this higher level of security and resilience in critical infrastructure sectors, there must be collaboration and information sharing.

"Collaboration is facilitated by establishing structures and processes necessary for government and the private sector to communicate freely without releasing proprietary information or providing unfair advantage; [it] support[s] a trusted information sharing environment where stakeholders share information to strengthen security and resilience."[309] At the cornerstone of critical infrastructure information sharing are these "established mechanisms or channels to reach stakeholders regularly, as well as before, during and after an incident."[310] These mechanisms not only make information sharing easier and more routine, but they also allow for the federal government to have "full and frank discussion with key stakeholders regarding sensitive vulnerability information."[311]

This information sharing and collaboration aspect of critical infrastructure is crucial to breaking down dangerous relationships between government and platforms. Government and society would no longer be completely beholden to the whims of platforms. While

[307] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 297, at 2; *see also* Exec. Order No. 13636, 78 Fed Reg. 11739 (Feb. 19, 2013).
[308] Goldsmith, *supra* note 14.
[309] CISA, *supra* note 306, at 11.
[310] *Id.*
[311] DEP'T OF HOMELAND SEC. OFF. OF THE PRESS SEC., *supra* note 299.

most of the critical infrastructure regime depends on voluntary cooperation, social media platforms would experience pressure from the government, other critical infrastructure sectors, and the public to cooperate through reporting and responding to information requests. The government also has increased authorities to assist and respond to threats faced by critical infrastructure entities—a benefit to both the private entity and the public. Another way to look at the relationship is that government and critical infrastructure entities become part of a team, a type of "treaty regime," with a shared goal to achieve security and resilience for the nation.[312] A more coterminous balance of power is reestablished between government and platforms by making them more akin to allies than opposing forces; they would have mutually reinforcing goals under the rubric of critical infrastructure. Ultimately, this may be a step toward tempering platforms from exercising exhausting levels of control over the speech environment and its users.

Information sharing and collaboration are also meant to facilitate a greater understanding of the threats to systems to quickly address them and keep systems running for public use. In other words, the information sharing regime can allow the government to carry out its duties of protecting the channels of expression and communication by ensuring they remain secure, operational, and safe for users. With information sharing comes a better understanding of threats facing the nation and users that government can begin to address through other means.

[312] Given the recent analogies of social media as its own form of governor or sovereign entity, one then might find some comparison to why nations obey international law: [N]ations obey international rules not because they are threatened with sanctions, but because they are persuaded to comply by the dynamic created by the treaty regimes to which they belong. "[T]he fundamental instrument for maintaining compliance with treaties . . . *is an iterative process of discourse* among the parties, the treaty organization, and the wider public." Harold Koh, *Review Essay: Why Do Nations Obey International Law*, 106 Yale L. J. 2599, 2601 (1997) (citing Abram Chayes & Antonia Handler Chayes, The New Sovereignty Compliance with International Regulatory Agreements 25 (1995).

For example, platform providers would likely want to, have to, or feel pressure to share information regarding foreign attacks to their user interface or security systems once they fall within the collaborative critical infrastructure framework. This could include threats such as foreign influence campaigns that threaten democracy and have the potential to cause civilian harm. Understanding these threats allows other national security mechanisms to work, such as the military, to address threats in foreign cyberspace to stop future threats from occurring.[313] Such coordination also helps lessen the impact of First Amendment implications at home. Information about these threats can be lost to the government without a collaborative information sharing regime with established mechanisms or channels to share information.[314]

The counterargument here, naturally, is that Congress already provided information sharing mechanisms between private entities and government through the Cybersecurity Information Sharing Act of 2015 (CISA), without the need for a critical infrastructure designation.[315] The Act provides private entities liability protection and mechanisms for information sharing with the government about "cyber threat indicators" and "defensive measures."[316] However, pursuant to CISA, threat indicators and defensive measures only include those cyber threats to networks and systems for cybersecurity protection.[317] While these threats are important to address for security purposes and data-related harms, it fails to include content-related information operation threats that might be solely violating an information platform's terms of service, for instance.[318] Moreover, the

[313] *See* KAPLAN, *supra* note 31, at 280-82 (noting U.S. CYBERCOM's mission of protecting critical infrastructure, which could be done in enemy territory after obtaining the information from platforms).
[314] *See also* discussion *infra* Part IV (discussing minimizing the privacy issues with information sharing with platforms).
[315] *See* Consolidated Appropriations Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015) ("CISA"); *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).
[316] CISA § 106; *see* S. Rep. No. 114-32, at 2-3 (2015).
[317] *See* CISA § 102 6-7.
[318] *See* S. Rep. No. 114-32, at 3-4 (2015); *see also* CISA § 102(5)(B).

private entity information sharing mechanisms set up through CISA's authority and construct are very limited and have its continued challenges.[319] For example, private entities must report their threat information through the Department of Homeland Security threat reporting system or else risk losing protections afforded under the Act.[320] Reporting to other government agencies, such as DoD or Department of State (including the Global Engagement Center),[321] would effectively strip private entities of CISA's protections. However, reporting to a critical infrastructure sector specific agency would not[322]—another potential benefit to social media platforms falling under a critical infrastructure designation.

As an alternative, one might argue that section 1642(b) of the fiscal year 2019 NDAA offers a route to more directly addressing information operation threats.[323] However, this authority too is problematic because there is nothing to indicate that private entities are inclined to enter into such voluntary sharing mechanisms.

---

[319] *See* OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY, UNCLASSIFIED JOINT REPORT ON THE IMPLEMENTATION OF THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 9-11 (Dec. 19, 2019), https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf (addressing continued challenges of implementing CISA for information sharing).

[320] CISA § 105(c)(1)(B)(i)-(ii).Under CISA, "the only way to receive the liability protection of section 106 is to share information through the 'DHS capability and process' created under section 105(c), or through the exceptions covering follow-up communications and 'communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.'" Brad S. Karp et al., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/. The designation of critical infrastructure would then open up an additional avenue for reporting to a sector specific agency, which would then be an exception for receiving liability protection when reporting outside the DHS system. *See id.*; CISA § 105(c)(1)(B)(ii).

[321] *See* Jenco, *supra* note 127

[322] CISA § 105(c)(1)(B)(ii).

[323] *See* discussion *supra* Part III.B.2 (discussing Section 1642 of the FY19 National Defense Authorization Act).

Needless to say, these available information sharing authorities still leave substantial gaps in addressing information warfare threats.

Besides, under the current structure of voluntary information sharing, platforms have no real incentive and are frankly disincentivized, to share information.[324] Congress' information sharing authorities established outside of the critical infrastructure mechanisms fail to address more pressing concerns private entities have regarding information sharing, and as a result, very few private entities participate.[325] Voluntarily sharing information about threats, for example, might provoke discussions among shareholders and the public that their systems are not safe or secure, inducing a public affairs nightmare for a company that wants to continue to grow and preserve profits. These fears arise from concerns that a company's private information may not remain so private when passed to the Federal entity, warranted or not.

In implementing a critical infrastructure rubric, shareholders would likely be less opposed to mandated disclosures that are encouraged by law through a more robust sharing framework that is monitored by a sector-specific agency lead with baked-in oversight mechanisms and a clear nexus to national security concerns.[326] On the flip side, government entities are also far more inclined to share with critical infrastructure entities important threat information and would

[324] *See* Goldsmith, *supra* note 14; Cordero, *supra* note 290 ("[E]ven under existing state laws and voluntary frameworks, companies are still disincentivized from providing transparency regarding data exposures or losses or other types of inadvertent accesses or manipulation, unless they are compelled by law to do so.").
[325] *See, e.g.*, Joseph Marks, *Only 6 Non-Federal Groups Share Cyber Threat Info with Homeland Security*, NEXTGOV (June 27, 2018), *https*://www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/; *see also* Khan & Pozen, *supra* note 175, at 497.
[326] *See* CISA, CRITICAL INFRASTRUCTURE THREAT INFORMATION SHARING FRAMEWORK: A REFERENCE GUIDE FOR THE CRITICAL INFRASTRUCTURE COMMUNITY (2016), *https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf.*

work harder to declassify important threat information.[327] The critical infrastructure designation ultimately makes it easier for each side to conceptualize the nexus to national security concerns. In the end, this relationship is more symbiotic, equal, and easy to grasp, especially more so than a fiduciary duty owed to users by platforms where the power dynamic between a platform and a single user is untenable and a duty is hard to define.

Creating a critical infrastructure relationship between platforms and government offers these sharing mechanisms that can serve as a step toward the government better understanding the full scope of platform information harms, including how platforms' business models and algorithmic control create such harms. As a result, there can be more informed policymaking decisions in the future for their regulation. Without these insights and collaboration, initial "peace talks" between platforms and governments cannot even begin.

IV. DATA

Although content is the obvious main attack vector for adversaries to maliciously access people for political ends, and hence the main focus of this article, there is still an underlying data problem that drives the information warfare machine in the United States. Part III of this article shows that the First Amendment may not be as much of a barrier to combating information warfare as assumed. In contrast, Part IV is meant to show the opposite when it comes to data. One of the most pressing obstacles to combating information warfare today is actually data business practices and the related individual privacy implications. As new technologies emerge and as the speech market begins to alter and, in some cases, go into the dark, we should be highly concerned about U.S. data practices. In the information age, data is

[327] *See* Robert K. Knake, *Sharing Classified Cyber Threat Information With the Private Sector*, COUNCIL ON FOREIGN REL. (May 15, 2018), *https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector.*

thought of as the "new oil" or raw material of our times.[328] As a corollary, in the information warfare context, data should be envisioned as both a resource and a new weapon.[329]

The information warfare problem has deep roots in U.S. data practices. The rendering of an individual's experience into data or "raw-material" through virtually every information platform or digital interface today is how adversaries get a foothold into gaining access to people.[330] Data drives profiling, targeting, and surveillance of individuals. All of these aspects then drive the data market.[331] Whereas data (or, more aptly "Big Data") can be a powerful public good in some respects and even help to secure our nation,[332] too much data flow combined with unregulated data practices and weak data security makes for a less secure nation—not only to information warfare but to a multitude of other related information harms.

---

[328] Joris Toonders, *Data is the New Oil of the Digital Economy*, WIRED (July 2014), https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/.

[329] *See* Nick Brunetti-Lihach, *Information Warfare Past, Present, and Future*, REAL CLEAR DEF. (Nov. 14, 2018), https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html.

[330] *See* ZUBOFF, *supra* note 97, at 234.

[331] *See id.* at 237 (discussing how terms of service and end user licensing agreements reveal oppressive privacy and security consequences in which sensitive information is shared with other devices, unnamed personnel, and third parties for the purposes of analysis and ultimately for trading in behavioral futures markets).

[332] *See* Jennifer Shkabatur, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354 (2019) (advocating for a global commons approach toward data use to take advantage of the social value of user-generated data to help solve a variety of public challenges instead of allowing the data to rest in the hands and control of a few powerful platforms); DOD DATA STRATEGY, UNLEASHING DATA TO ADVANCE THE NATIONAL DEFENSE STRATEGY 3 (Sept. 30, 2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF (identifying data as a strategic asset); *see also* Randy Bean, *Another Side of Big Data: Big Data For Social Good*, FORBES (Sept. 23, 2016) ("Big Data is a double-edged sword, bringing insight, while also posing risks to privacy or abuse when data falls into nefarious hands.").

A. The Underlying Data Problem: Data Fuels the Information Warfare Machine

"Every discussion of data protection or data ownership omits the most important question of all: why is our experience rendered as behavioral data in the first place?"
Shoshana Zuboff, The Age of Surveillance Capitalism[333]

Cambridge Analytica is almost synonymous today with the term information warfare. The scandal was highly publicized from congressional hearings to the court of public opinion.[334] Millions of social media users' data were surreptitiously accessed and exploited to disrupt and manipulate the 2016 U.S. presidential elections.[335] Between 2013 to 2015, researchers working with Cambridge Analytica harvested Facebook profiling data and used Facebook's targeted advertising tools to build psychological profiling algorithms.[336]

---

[333] *See* ZUBOFF, *supra* note 97, at 233.

[334] *See Cambridge Analytica and the Future of Data Privacy, S. Comm. on Judiciary*, 115th Cong. (2018).

[335] *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Facebook applications that were originally developed for an academic purpose would capture not only the original application user data but would also harvest all the personal data of that user's Facebook friends and connections – without their knowledge or explicit consent – and was provided to Cambridge Analytica. *Cambridge Analytica and the Future of Data Privacy, Statement of Christopher Wylie Before S. Comm. on Judiciary*, 115th Cong. 6 (2018) [hereinafter *Wylie Statement*]. Facebook later confirmed that the lead researcher did not have permission from Facebook to exploit the app's privileged access for commercial or political activities. In the end, approximately 80 million users' data, most of which was American was exploited.

[336] *See Wylie Statement* at 5-6 (discussing how the work of Cambridge Analytica was not equivalent to traditional marketing; it specialized in disinformation, spreading rumors, kompromat and propaganda" using machine learning algorithms); ZUBOFF, *supra* note 97, at 280-81; Cadwalladr & Graham-Harrison, *supra* note 335; Carole Cadwalladr, *The Cambridge Analytica Files: 'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, GUARDIAN (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Cambridge Analytica then exploited the information to target users' "inner demons"—identifying and narrowly targeting mental and emotional vulnerabilities in subsets of the American population—to advance the political agendas of its clients in the 2016 U.S. elections.[337] Whistleblower, Chris Wylie, described Cambridge Analytica's tactics as nothing less than "information warfare."[338] He labeled the practices fundamentally "not conducive to democracy."[339] In sum, the scandal showed how the data practices of the platform economy could be turned into a strategic information warfare weapon used to directly target society on social media for political ends.[340]

What is most concerning about Cambridge Analytica is that these practices were not novel uses of personal data;[341] there was no massive data breach to speak of in a traditional sense,[342] and there was nothing inherently illegal about what the company or the platform did.[343] Facebook claimed it followed its permissible data business practices—it was all standard procedure.[344] Cambridge Analytica, on the other hand, merely used the data market, behavioral profiling, and microtargeting to its advantage in the political sphere.[345] To most Americans, however, it was the first real glimpse of how their most

[337] *Wylie Statement* at 5-6, 9 ("Cambridge had direct links to Russia and worked openly with Russian-linked companies to share information on 'rumour campaigns' and 'attitudinal inoculation.'"); Cadwalladr & Graham-Harrison, *supra* note 335.
[338] Cadwalladr, *supra* note 336.
[339] *Id.*
[340] *See, e.g.*, Terry Gross, *Whistleblower Explains How Cambridge Analytica Helped Fuel U.S. 'Insurgency'*, NPR (Oct. 8, 2019), https://www.npr.org/2019/10/08/768216311/whistleblower-explains-how-cambridge-analytica-helped-fuel-u-s-insurgency.
[341] *Statement of Mark Jamison Before the S. Judiciary Comm., Politics and Business in Social Media*, *supra* note 155, at 2.
[342] *See* Cadwalladr & Graham-Harrison, *supra* note 335 (discussing Facebook's denial of a data breach in the case of Cambridge Analytica).
[343] *See id.* Although some contest that the researchers violated platform terms of service, Facebook failed to be completely clear and have understandable terms. *See Statement of Mark Jamison Before the S. Judiciary Comm., Politics and Business in Social Media*, *supra* note 155, at 4, 6.
[344] *See* Cadwalladr & Graham-Harrison, *supra* note 335; Cadwalladr, *supra* note 336.
[345] *See* ZUBOFF, *supra* note 97, at 281; *see also Wylie Statement* at 5-6 (discussing the effectiveness of profiling, backed by copious amounts of peer-reviewed literature).

private human experiences were being mined, cultivated, and covertly used against them. U.S. data protection and consumer protection laws really have nothing to say about it.

Cambridge Analytica tells the story of how U.S. data practices are at the heart of information warfare. The company did not just troll social media platforms to find polarizing divisions within society, rather they went deeper in the mining of Americans' data to carry out its targeting. Cambridge Analytica (notably, a non-U.S. company based in the U.K.) mined data through the platform (i.e., Facebook) and applications to develop and scale its own malicious psychological profiling algorithms.[346] The company's mass sensitive data collection and data handling practices, coupled with connections to adversarial foreign agencies, also presented a gross risk of data breaches and foreign intelligence gathering that could fuel additional foreign information warfare campaigns.[347] So, while some may argue that adversaries can just find polarizing divisions within society directly from social media without the underlying data, the most malicious and effective forms of information warfare will be from actors accessing and harvesting personal data for their nefarious uses to target deeper and more intrusively.

These types of data abuses are not limited to grand political schemes either. Today, data is for sale, including the mining of it, to virtually anyone who is in the market to buy it. Private entities,[348] the

[346] *See id.*; Gross *supra* note 340.
[347] *See Wylie Statement* at 9.
[348] *See, e.g.*, Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

U.S. government,[349] foreign companies and governments,[350] and various nefarious actors are in that market. Even U.S. government agencies tagged with the sole responsibility for countering information warfare efforts are "data-driven" market participants looking to data as a solution, rather than a root problem.[351] Or, perhaps those agencies look to data because others look to data, thereby kicking off a data arms race. Millions of Americans' data is sold and used daily, predominately without their knowledge through the use of platforms or digital applications on platforms and devices.[352] Multiple recent

[349] *See, e.g.*, Mitchell Clark, *US Defense Intelligence Agency Admits to Buying Citizens' Location Data*, VERGE (Jan. 22, 2021), https://www.theverge.com/2021/1/22/22244848/us-intelligence-memo-admits-buying-smartphone-location-data; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Forret Milburn, *Facebook May Not Sell the Data it Collects, But the State of Texas Sure Does,* HOUSTON CHRONICLE (Apr. 13, 2018), https://www.houstonchronicle.com/politics/texas/article/Facebook-may-not-sell-the-data-it-collects-but-12832831.php; Editorial Board, *Apps are Selling Your Location Data. The U.S. Government Is Buying*, WASH. POST (Feb. 9, 2020), https://www.washingtonpost.com/opinions/apps-are-selling-your-location-data-the-us-government-is-buying/2020/02/09/9d09475e-49e2-11ea-b4d9-29cc419287eb_story.html.

[350] *See* WHITE HOUSE, EXECUTIVE ORDER ON PROTECTING AMERICANS' SENSITIVE DATA FROM FOREIGN ADVERSARIES (June 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/ (discussing the threat of U.S. personal data being sold or acquired by adversarial foreign governments that poses a threat to national security).

[351] *Hearing Before the Subcomm. on State Department and USAID Management, International Operations, and Bilateral International Development of the S. Comm. on Foreign Rel.* (statement of Lea Gabrielle), 7-8 (stating, "At the [Global Engagement Center] (GEC), we have an emphasis on making sure we are data-driven. There is an increasing demand from our U.S. government and foreign partners for data analytics and targeted advertising technologies to counter propaganda and disinformation."); *see also* Clark, *supra* note 349.

[352] *See, e.g.*, Valentino-DeVries et al., *supra* note 348; Geoffrey A. Fowler, *I found your data. Its's for sale*, WASH. POST (July 18, 2019), https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/; Douglas MacMillian, *Data Brokers are Selling Your Secrets. How States Are*

exposés about the data market by major news outlets showed just how prevalent, lucrative, and concerning the data market has become.[353]

Concerns over private data practices and the growth of an unregulated market were not completely lost on Congress before Cambridge Analytica or such media exposés. In early 2018, members of Congress took note when the use of personal health and fitness data collected by an exercise application and platform, Strava, aggregated and publicized millions of data points that ended up revealing concentrations of military personnel and locations.[354] Members of the U.S. House of Representatives Committee on Energy and Commerce expressed concerns with the company about exposing the identities of military personnel and locations, the possibility of deanonymizing data to identify specific individuals, and the extent of data sharing with third parties.[355]

More recently, Congress turned its attention to the antitrust issues involved in online platforms and market power, with a major focus on the role of data practices.[356] Although congressional hearings addressing these issues are a step in the right direction, solving information harms through antitrust laws nearly misses the mark when it specifically comes to information warfare.[357] In many

Trying to Stop Them, WASH. POST (June 24, 2019) https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/; *see also* Sam Schechner, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[353] *See* CISA § 105(c)(1)(B)(i), (ii).

[354] DENARDIS, *supra* note 148, at 73-74.

[355] *Id.*

[356] *See generally Digital Markets Investigation: Antitrust Investigation of the Rise and Use of Market Power Online and the Adequacy of Existing Antitrust Laws and Current Enforcement Levels*, *Hearings Before H. Comm. on Judiciary*, 116th Cong. (2019-2020).

[357] However, the antitrust issues regarding the aggregation of power by a select few information platform companies is a powerful counterargument to the assumption that unregulated data practices are necessary in the United States to drive competition and require "permissionless innovation." Tom Wheeler, *Digital*

instances, antitrust laws will not solve the information warfare problem because it is typically the smaller third-party companies that are using platforms to their advantage to buy or harvest personal data, especially through targeted advertising.[358] This is the aspect that most Americans and policymakers have little insight about today and is another reason to push for increased information sharing with social media platforms and the government about underlying practices.

In light of Congress' growing interest in the data market and practices, and such scandals as Cambridge Analytica, Americans are becoming more attuned to information harms in the United States caused by the platform economy. The tides may finally be turning away from a public tolerant of corporate data collection and surveillance.[359] A 2019 Pew Research Center report found "some 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits."[360] Yet, despite this rising healthy skepticism, the majority of Americans still feel they have little control over the data collected about them or lack an understanding of how their data is being used.[361] Data practices make Americans feel helpless instead of tolerant. As the report showed, "roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life without having data collected about them by companies or the government."[362] This says a lot about the true nature

Competition with China States with Competition at Home, BROOKINGS (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_digital_competition_china_wheeler_v3.pdf.

[358] Facebook is a consumer of data, driving the data market, which entices smaller third-party platform-based applications to collect data and sell to Facebook. *See* Schechner, *supra* note 352.

[359] *See* Sheldon Whitehouse, *Why Americans Hate Government Surveillance but Tolerate Corporate Data Aggregators*, LAWFARE (June 2, 2015), https://www.lawfareblog.com/why-americans-hate-government-surveillance-tolerate-corporate-data-aggregators.

[360] Brooke Auxier et. al, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[361] *Id.*

[362] *Id.*

of informational autonomy or informational self-determination today. It also speaks volumes about how much consent we have or whether we truly have choices in "subscribing" to the new public square.

Unfortunately, the data market and abusive practices are only one-half of the problem. Not only is data for sale—and by a whole host of entities—but lax company cybersecurity and government enforcement also make data prone to theft and exploitation. In 2014, for example, Chinese hackers stole the personal data of more than twenty-one million people from the U.S. Office of Personnel Management.[363] When combining cybersecurity problems with data practices, the information warfare problem is exacerbated. Although companies note that information obtained "legally" within the market might be anonymized to buyers, anyone with access to the raw data—including employees, clients, hackers, or nation state intelligence operations—could still identify a person without consent.[364] Professor Paul Ohm makes this point in his research, suggesting that the amalgamation of raw data and anonymized data can easily be used to rebuild specific identities and individual profiles of people.[365]

These issues stress another key aspect of the data problem related to information warfare: not only is data used to find general divisions in society, but it is also used for direct individualized targeting of key decision-makers on a more personalized basis. In the military context, the personal data of individuals may be considered an emerging attack vector in its own right for the conduct of future operations in today's information environment.[366] This type of highly

[363] *See In re*: U.S. Office of Personnel Management Data Security Breach Litigation, 928 F.3d 42, 49-50 (D.C. Cir. 2019).
[364] Valentino-DeVries et al., *supra* note 348.
[365] *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).
[366] Christopher K. Dearing, *Personal Information as an Attack Vector: Why Privacy Should Be an Operational Dimension of U.S. National Security*, 10 J. NAT'L. SECURITY L. & POL'Y 351 (2020).

individualized attack driven by data access, collection, and exploitation will likely become the future of information warfare.

Increasing amounts of evidence also suggest that bad actors are shifting information warfare campaigns from open platforms like social media to encrypted messaging applications that work across platforms.[367] In the years to come, individuals may be inclined to shift to more closed platform applications due to the perception of private and government surveillance through data collection practices.[368] Additionally, such closed applications that work across platforms like WhatsApp, for example, present challenges for identifying and responding to information warfare campaigns targeted to specific users and give users the perception of a more trusted medium, features that bad actors find enticing.[369] In such a closed environment, the effectiveness and ability to utilize techniques such as marking disinformation or using counternarratives to lessen information warfare harms will be greatly diminished, if not completely useless.

More direct, individualized, and intrusive targeted attacks that gain access through personal data, therefore, should be viewed as the future of information warfare. This shift in practice is already underway. During the early months of the novel coronavirus pandemic, individuals started to receive disinformation about the virus via closed message applications.[370] The United States must keep

---

[367] *See* Senator Mark R. Warner, *White Paper: Potential Policy Proposals for Regulation of Social Media and Technology Firms* 2 (2018).

[368] *See Encrypted Messaging: What Is It, Why Should You Use It and What Are the Best Apps?*, PIXEL PRIVACY (last accessed May 15, 2020), https://pixelprivacy.com/resources/encrypted-messaging/ (advocating for the use of encryption technology because of increasing government surveillance techniques); *see generally* Warner, *supra* note 367 at 2; Alex Shephard, *A Long Overdue Blueprint Regulating Big Tech*, New Republic (July 31, 2018), https://newrepublic.com/article/150337/long-overdue-blueprint-regulating-big-tech.

[369] *See* Warner, *supra* note 367, at 2.

[370] Mihir Zaveri, *Be Wary of Those Texts From a Friend of a Friend's Aunt*, N.Y. Times (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/us/coronavirus-text-messages-national-quarantine.html; *see also* Edward Wong et al., *Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say*, N.Y. Times

these growing tactics in mind with the emergence of the internet-of-things—a world we currently live in—where access and control of personal data will gain even more importance as we merge our cyber and physical worlds.[371] The ability to access and target trusted and intimate areas of individuals' daily lives becomes even more acute and ominous.

B. The Data Privacy Legal Framework: A Loosely Regulated Environment

In 2018, Carrie Cordero, Adjunct Professor and Senior Fellow at the Center for a New American Security, gave the keynote speech at the Georgetown Cybersecurity Law Institute to discuss emerging cybersecurity issues.[372] The event was open to both the legal and corporate communities.[373] Professor Cordero's main premise was that America needed to start connecting the dots between corporate data collection and U.S. national security threats.[374] Professor Cordero recently recalled that the topic did not go over well with a room half full of private-sector technology company representatives.[375] Since what she was advocating suggests altering the core business practices of many of those companies, this comes as no surprise.[376] Perhaps of most consequence, though, is that not much has changed over the past few years in our legal landscape to start protecting our national security interests when it comes to data practices. Paradoxically, this

(Apr. 22, 2020), https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.

[371] *See generally* DENARDIS, *supra* note 148.

[372] Cordero, *supra* note 290.

[373] *Id.*

[374] *Id.*; *see also* Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation is Just A Start*, BROOKINGS (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/ (arguing that data practices and individual privacy is a national security concern).

[375] Conversation with Carrie Cordero, Senior Fellow at the Center for a New American Security, in Andrews Air Force Base, Maryland (Mar. 3, 2020).

[376] *See, e.g.*, Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 11 (2019) ("Data harvesting and processing are one of the principle business models of informational capitalism.").

is one area of the law where looming national security threats—most especially information warfare—demand *more* individual privacy.[377] Despite this growing acknowledgment, we are still facing a largely "loosely regulated environment."[378]

The American privacy legal landscape is complex and scattered. Often this landscape is best described as a patchwork of sectoral, industry-specific, and state-based consumer and data protection privacy laws.[379] For this reason, it is perhaps best to start with an overview of the U.S. privacy legal landscape by juxtaposing it against the European Union (EU)—to show what U.S. privacy law is not, as well as what is currently driving "a tidal wave of public support for a privacy law revolution" in America.[380]

In 2016, the EU approved the General Data Protection Regulation (GDPR), a comprehensive privacy law that took effect in

[377] One might compare this situation to post 9/11 and the fight against terrorism, where many citizens gave up significant privacy rights in the name of national security, such as through the enactment of the USA/PATRIOT Act that increased the scope of permissible government surveillance. *See* Laura K. Donohue, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL WORLD 24-26 (2016).

[378] Cordero, *supra* note 290.

[379] WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 257 (2016); *see* Eric Rosenbach & Katherine Manstead, *How to Win the Battle Over Data*, BELFER CTR. (Sept. 17, 2019), https://www.belfercenter.org/publication/how-win-battle-over-data. "A U.S. company could contend with more than 50 different overlapping and sometimes contradictory data laws, which together are still insufficient to ensure basic data governance and protection standards." With regard to government data collection and processing, the Privacy Act of 1974 is meant to provide certain safeguards to individuals against invasions of privacy by the federal government by protecting against the misuse of government records and providing individuals with more control of agency information about themselves. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974). The major problem with the Privacy Act is that it has largely transformed over the years into "box-checking exercise rather than a substantive check on the government's power." Rachel Levinson-Wallman, BRENNAN CENTER FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 49 (2013).

[380] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV., 5 (2020) ("[C]hange is now on America's doorstep.").

May 2018 and replaced the previous 1995 EU Data Protection Directive.[381] The EU GDPR is based on a comprehensive data protection model. Ironically, this data protection model is based on the fair information practices (otherwise known as the FIPs) that were significantly developed by the U.S. government in the 1970s, yet far less influential in the United States.[382] Most data protection laws such as these provide people with affirmative rights.[383] Additionally, in the EU, privacy rights originate in the individual's inherent control over personal information, classified as a human right.[384] Europe's recognition of fundamental human rights to privacy and data protection, therefore, provides protection against both governments and private actors.[385]

By contrast, the United States' predominant consumer protection privacy model does not follow this general model of data protection (except in limited cases) or consider privacy a human right. Under the U.S. Constitution and statutory law, there is no explicit constitutional right to privacy.[386] Privacy in the United States is only implicitly protected as a negative right against the government—not private actors—in a few areas, including: "First Amendment right to anonymous expression, the Third Amendment protection against the quartering of soldiers in private homes during peacetime, the Fourth Amendment's 'reasonable expectation of privacy' against government searches and seizures, and Fifth and Fourteenth Amendment substantive due process rights to information privacy and decisional autonomy."[387]

As a result of this structure, U.S. consumer privacy and data protection rules developed as the implementation of public policy, not

[381] *What is GDPR, the EU's new data protection law?*, https://gdpr.eu/what-is-gdpr/ (last visited Mar. 20, 2020).
[382] *See* Hartzog & Richards, *supra* note 380, at 1701-02; MCGEVERAN, *supra* note 379, at 257.
[383] *See* Hartzog & Richards, *supra* note 380, at 1701-02.
[384] *Id.*
[385] *Id.* at 1727-28.
[386] *Id.*
[387] *Id.*

for the vindication of fundamental rights.[388] In practice, this means the main protections and enforcement mechanisms for individual privacy and data protection in the United States under the Federal Trade Commission Act, which prohibits unfair and deceptive consumer trade practices, are not compelled by the protection of fundamental rights.[389] Privacy is just one interest balanced in the policy discussions that shape such rules.[390] Consequently, legal reform aimed at data practices and data privacy that are compelled by policy may offer an easier inroad to protecting access to people when compared to reforming laws aimed at controlling content that implicate the First Amendment and are compelled by the protection of fundamental rights.[391] Still, one major roadblock remains: policy discussions that shape privacy rules historically favor other U.S. values and interests over individual privacy. This favoritism is the root of the American privacy and data problem and why there is such a loosely regulated framework. Our conception of this policy balancing act in light of today's threats may, however, no longer be suitable for the

[388] *Id.*

[389] Hartzog & Richards, *supra* note 380, at 1727-28. There is considerable concern about the Federal Trade Commission's (FTC) ability to actually enforce data practices. Compare *In re Dave & Buster's Inc.* FTC Docket No. C-4291 (June 8 2010) and *LabMD, Inc. v. Federal Trade Commission*, 891 F.3d. 1286 (11th Cir. 2018) (highlighting the purpose of consumer enforcement actions in relation to cybersecurity practices and putting the future efficacy of FTC consent decrees into question). However, there are some advantages to the FTC as an enforcement authority. The FTC's consent decrees create what some academics recognize as a whole jurisprudence in America about what constitutes reasonable data practices. *See generally* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019). The FTC also creates relationships with agencies through decrees that is beneficial in times of changing technology. *See generally* William McGeveran, *Friending the Privacy Regulators,* 58 ARIZ. L. REV. 959 (2016).

[390] Hartzog & Richards, *supra* note 380, at 1730.

[391] *But see* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63-64 (2014) (arguing that data, to include personal data, does and should receive First Amendment protections because it creates knowledge). *But cf.* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 86-87, 90 (2015) (arguing that treating commercial data flows as speech protected by the First Amendment is inconsistent with the free speech doctrine and interferes with other important values).

information environment, especially for preserving the security of the individual as well as the nation.

C. Reconsidering Data Privacy Policy: Weighing Innovation, Competition, and Democracy

After the Cambridge Analytica scandal broke in 2018, the Senate Judiciary Committee held hearings to discuss the aftermath and the future of data privacy in the United States.[392] Professor Mark Jamison advocated against further regulation of platforms and data protection.[393] His arguments are used here to summarize some of the prevailing policy arguments advanced for why the United States should maintain a "loosely regulated environment" for data privacy.

The first argument is that regulation of data will stifle innovation. According to Jamison, Facebook merely made a mistake with Cambridge Analytica, and such mistakes are a result of innovation.[394] He suggests restricting Facebook would be futile, would damage a dynamic tech economy and the future of innovation, and that existing law can address the situation to prevent future abuses.[395] Further, Jamison claims that attempts to make such business mistakes in the handling of personal data illegal would make it worse because businesses have better information on what customers value than do government regulators—making the free market the better disciplinarian than a less-informed regulator.[396]

---

[392] *Cambridge Analytica and the Future of Data Privacy, S. Comm. on Judiciary*, 115th Cong. (2018).
[393] *Id.*; *Politics and Business in Social Media*, *supra* note 155 (statement of Mark Jamison).
[394] *Politics and Business in Social Media*, *supra* note 146, at 7(statement of Mark Jamison).
[395] *Id.*
[396] *Id.*

While it may be true that relaxed or permissive data privacy rules helped build Silicon Valley,[397] the emerging trade-offs no longer make this a viable path to achieve innovation (or, for that matter, competition).[398] American policymakers must question how virtuous and productive innovation has become when it now plays a large part in the deterioration of both individual privacy and national security. The policy trade-offs can no longer be viewed as merely individual harms that involve the loss of privacy; the policy trade-offs must also involve public harms such as threats to national security and democratic ideals.[399] As Professor Cohen cautions, "the cultural and political discourses that have emerged around data-centered 'innovation' work to position such activities as virtuous and productive, and therefore ideally exempted from state control."[400] This prevailing discourse led to the current regulatory scheme that allows for companies and private actors to have a vast amount of discretion in how they handle the personal data of Americans, all for the achievement of the "public good of mass data collection" that presumably drives innovation or competition.[401] Such discretion, however, continues to lay the essential groundwork for cultivating national security threats in the information environment with the nearly unfettered datafication of our everyday lives. As these data practices are allowed to proliferate, the nation and individuals become

[397] *See* Chander, *supra* note 155, at 664-68. Cf. Tom Wheeler, *A Focused Federal Agency is Necessary to Oversee Big Tech*, BROOKINGS (Feb. 10, 2021), https://www.brookings.edu/research/a-focused-federal-agency-is-necessary-to-oversee-big-tech/ ("Taking advantage of policymakers' inaction, digital companies assumed a pseudo-government role to impose their own will on the digital marketplace[, which has] failed to adequately protect both the rights of consumers and the benefits of competition.").

[398] *See generally* Wheeler, *supra* note 397.

[399] As noted in Part II, policymakers need to make more symmetrical policy arguments for reform by comparing public advantages (i.e., mass data collection that drives innovation) to corresponding public harms (i.e., global fatalities (in the case of health disinformation especially), increasing national security risks, and the deterioration of our democracy), rather than hyper-focusing on individual level harms. *See* DENARDIS, *supra* note 148, at 88.

[400] *See* Cohen, *supra* note 376, at 11; Wheeler, *supra* note 397 (discussing this innovation and competition discourse against regulation as the "policy con").

[401] *See* Wheeler, *supra* note 397.

exceedingly more vulnerable to exploitation by creating vectors for attack through data.

Moreover, evidence shows that the majority of the body politic feels exploited by current data practices—belying the argument that businesses have better information on what customers value. Yet, individuals feel helpless to effectuate change because of the power disparity with platform providers. Individuals feel trapped into using such services to carry out their daily lives.[402] A marketplace is developing that looks quite unlike one that can interpret what customers value. Rather, the marketplace is turning into an environment where platforms or tech companies can exploit their position to the detriment of communities dependent on them, all in the name of innovation.[403]

Such power disparities and resulting exploitation of the public is not an unfamiliar situation for the United States. Public utilities were regulated for these very reasons.[404] Food safety also became regulated for similar reasons, most of which was because consumers could not observe food safety before consumption.[405] In our current data environment, users similarly cannot observe the security or safety of their data throughout its lifecycle once it is in the hands of platform providers, data brokers or, even in some cases, the government. The majority of users have little to no idea how their data is being used and later exploited, nor do they understand what security or precautions are being taken to protect them.[406] American policymakers determined in years past that these are the exact situations where government regulation needs to step in to temper the overwhelming drumbeat of "innovation" and progress.[407]

---

[402] *See* Auxier et. al, *supra* note 360.
[403] *See Politics and Business in Social Media*, *supra* note 155 at 3 (statement of Mark Jamison)
[404] *Id.* at 4-5.
[405] *Id.*
[406] *See* Auxier et. al, *supra* note 360.
[407] *Politics and Business in Social Media*, *supra* note 155 at 5 (statement of Mark Jamison)

Second, related to innovation, Jamison claims that data regulation will induce less competition. In making this claim, Jamison compares the GDPR and how its broad application will impede freedom, stifle innovation, and raise costs, which will lessen competition and result in harm to customers.[408] Jamison's claims, however, fail to account for the fact that the GDPR is already driving a privacy revolution in America. Companies in the United States already find themselves having to comply with the GDPR because of its extraterritorial scope.[409] The GDPR protects data subjects located in the EU, but if a U.S. company collects any personal data of someone located in the EU (regardless of citizenship or nationality) then it must comply with the GDPR.[410] Most global technology firms, such as major social media platforms like Facebook, have business practices that trigger the application of the GDPR.[411] The GDPR's protections and the daylight given to mounting data abuses even spurred American states to act. California is a prime example as it recently passed its own privacy law to ensure greater data protection for its residents, which is having a similar national effect on large interstate companies.[412] This is to say that the GDPR is not a case to avoid; it is already our current reality. Instead of looking to prevent something like the GDPR, the United States should instead focus on finding its place within privacy's already ongoing "constitutional moment."[413]

This leads to another reason why Jamison's assertions, and others like it, have strong counterpoints. In supporting the claim to avoid regulation like the GDPR to preserve innovation and competition, Jamison cites in part to a study showing that companies with the capacity to separate and migrate data are moving quickly to transfer customers' data physically located in the EU onto serves in the

[408] *Id.* at 7-8.
[409] Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 3.
[410] MCGEVERAN, *supra* note 379, at 21.
[411] *See id.* (Noting international companies would satisfy either the "establishment" requirement under Article 3(1) or the "targeting" provisions under Article 3(2)).
[412] *See* California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100-1798.199 (West 2021).
[413] *See generally* Hartzog & Richards, *supra* note 380, at 3.

United States.[414] Implicit in this assertion is that more companies will be lured to do business in America because of its permissive regulatory environment. Underlying this suggestion, however, is that companies are really driven to America because the raw material remains easier to harvest here; U.S. laws simply expose Americans—their data—to exploitation. Viewing this end result as good for competition, rather than a devasting blow to security, is concerning. If this is the argument in favor of competition and innovation, then the balancing act for U.S. policy objectives is askew. Privacy laws and regulations should not create loopholes for U.S. citizens' data to be targets because it is more accessible and vulnerable than citizens or residents of other countries.

Another argument to support the notion that regulation will stifle competition, again summarized by Jamison, is that the most appropriate way to address concerns about the concentration of data in the hands of a few is to make it easier to compete with these companies, not additional regulation.[415] Jamison posits, "[e]xisting and upstart companies will become more competitive in the digital marketplaces if public policy removes barriers to the profitability of deploying information technologies and networks."[416] To argue this point, Professor Jamison uses 5G networks as an example of regulation potentially standing in the way of competition and innovation.[417] The 5G example, however, is somewhat of a red herring in this context of data proliferation and abusive business practices. Regulation in the network infrastructure space—already minimal for private companies—primarily exists to ensure critical security of globally interconnected networks and infrastructure, as well as liability for data breaches. These regulatory efforts effectively secure data and control malicious access to it. The issue 5G network proliferation and regulation raises is more of a cybersecurity issue, an interrelated

[414] *Politics and Business in Social Media*, *supra* note 155 at 8 (statement of Mark Jamison) (citing to a 2018 study conducted by Shane Tews, American Enterprise Institute).
[415] *Politics and Business in Social Media*, *supra* note 155, at 5 (statement of Mark Jamison).
[416] *Id.*
[417] *Id.*

problem that also requires far more regulation to secure the nation vice less regulation.[418]

These arguments also show that policymakers need to interrogate such claims about the regulation of our data and data-related technology use by the private sector on a more granular level and determine what the data is, how it could be used against us, and who it is going to and why. Regulating data in one area may have graver consequences than regulating data in another (e.g., technical infrastructure data verse personal data). Regulating different types of data differently is a concept the United States should already be familiar with due to its sectoral privacy approach.[419] It is not, and should not be, a one-size-fits-all solution when weighing privacy, national security, competition, and innovation.

A final consideration for the policy debate is the effect on democracy. Current U.S. policy and law surrounding data practices hamper democracy, and therefore, impair national resiliency as a body politic to fend off the effects of information warfare. Considering this method of war is meant to destroy democracy, America should do all that it can through law and policy to restore democratic ideals and its centrality in the lives of Americans.

Democracy is stifled by American data practices and its interaction with the emergent platform economy because it drives surveillance. American data practices created a lucrative market for the buying and selling of personal information. That market developed into what Shoshana Zuboff refers to as surveillance

[418] This article's focus on a data-centric solution to information warfare by no means suggests neglecting network-centric efforts. On the contrary, cybersecurity and data security need to be viewed as mutually reinforcing mechanisms to solving the information warfare problem. Discussing the needed reform and issues revolving around cybersecurity is, however, outside the scope of this article.

[419] For instance, Congress has provided more protections for health-related data and financial data in specific situations. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 (104th Cong. 1996); The Gramm-Leach-Bliley Financial Services Modernization Act, 15 U.S.C. §§ 6801 et seq. (2010); The Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. (2012).

capitalism or the framework of a surveillance economy.[420] While private entities do the surveillance that is required for their data harvesting,[421] there are few barriers to the government also benefiting from that data as a market buyer. Essentially then, private surveillance drives government surveillance and vice versa. Without clear laws or regulations in place restricting data flows to all sources, the current legal framework provides the platforms (or the new speech moderators), private third parties, government, and foreign adversaries the freedom to participate on a nearly unrestricted basis in the surveillance market.[422]

Needless to say, surveillance by the government is a quintessential Fourth Amendment and individual privacy concern. The Fourth Amendment was founded on the notion of securing a person from general unreasonable searches and seizures by the government and a requirement for specific warrants,[423] which later developed through legal precedent to include unreasonable government surveillance.[424] Similarly, it can animate the Third Amendment that also makes up the zone of privacy, in that unwarranted surveillance in a person's home is analogous to having a police officer quartered in your home during peacetime—able to have access to your most intimate conversations and sphere of daily life.[425] Professor Brennan-Marquez, among other scholars, articulated the foundations for this concern in the Fourth Amendment: surveillance

[420] ZUBOFF, *supra* note 97, at 233.
[421] *See id.* at 235 (arguing there is no surveillance without rendition of data).
[422] In general terms, under Fourth Amendment jurisprudence the government can typically have access to anything within public view or provided to third parties, the argument being that there is then no reasonable expectation of privacy to protect under the Fourth Amendment. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40-41 (1988); Smith v. Maryland, 442 U.S. 735 (1979). *But cf.* Carpenter v. United States, 138 S. Ct. 2206 (2018) (carving out an exception under the third-party doctrine).
[423] *See* Laura Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1193 (2016).
[424] *See* Berger v. New York, 87 S. Ct. 1873 (1967) (extending the Fourth Amendment protections to electronic surveillance via wiretapping).
[425] *Cf. id.* at 1886 (Douglas, J., concurring).

stunts autonomy and modern political thought.[426] Likewise, it chills the exercise of civil liberties, especially those related to expression and association when individuals believe they are constantly being surveilled.[427] "For the same reasons that surveillance diminishes individual autonomy, it imperils collective autonomy—it hobbles democracy."[428] Put differently, "[s]tunted selves do not make for a healthy body politic."[429]

But this concern goes for any type of constant surveillance, especially if it may end up in the hands of speech moderators, the government, or more importantly in the hands of adversarial foreign governments. As Professor Brennan-Marquez argues, "when a polity becomes accustomed to (1) constant surveillance of daily life, coupled with (2) knowledge that the government will ultimately have access to the fruits of that surveillance, democracy wilts."[430] Our resiliency to fend off attacks on our democracy becomes weaker as our trust in the government is attacked from all sides. Thus, to restore and strengthen our notion of democracy, Professor Brennan-Marquez suggests that the constraints on private surveillance should take conceptual cues from the constraints that Fourth Amendment law has traditionally placed on state surveillance.[431] Such a suggestion, of course, demands us to reconceptualize and make drastic reforms to our current laws and policies surrounding privacy and data practices. Admittedly, this is a monumental challenge, but if this argument is correct, then our democracy depends on it.

[426] Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485, 494 (2018) (discussing the potential application of the state action doctrine to private surveillance).
[427] *Id.*; Neil M Richards, *Privacy and Technology: The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).
[428] Brennan-Marquez, *supra* note 426, at 496.
[429] *Id.*
[430] *Id.* at 498.
[431] *Id.* at 519.

D. Contemplating a Data-Centric Approach to National Security

Moving to a data-centric approach to national security may still be a grassroots sentiment within national security circles. The push for more consumer control over data by privacy and civil liberty advocates, as well as pressure from the EU and other states to adopt GDPR-style data protection regimes, moves this data-centric approach forward. Any GDPR-style legislative response in the United States, however, will have to take into consideration the civil liberties of the companies.[432] Despite the benefits and attractiveness of a GDPR-like statute to combat privacy harms and data security concerns, it might ultimately fail in America if adopted wholesale. The U.S. consumer-based privacy framework, for better or for worse, works to balance other constitutional rights, such as the First Amendment.

These obstacles should not stop much-needed reform. Again, the First Amendment is not a complete roadblock to regulation. Professor Neil Richards also argues this point. Getting sidetracked by the First Amendment, he contends, is dangerous because the costs of not regulating commercial data trade are significant.[433] Regulating these commercial data flows is not off-limits, rather the government can regulate this area if it acts rationally to further a legitimate government interest and that interest is sufficiently narrowly tailored.[434] Qualifying legitimate government interests have been

---

[432] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 900 (2010) (quoting First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 784 (1978)).

[433] RICHARDS, *supra* note 427, at 90.

[434] *See, e.g.*, Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001) (finding the FCRA survives intermediate scrutiny). *Cf.* Sorrell v. IMS Health Inc., 564 U.S. 552, 572 (2011). First Amendment concerns are precisely the reason why a complete ban on targeted advertising would not pass constitutional scrutiny. While some might think the harms associated with behavioral micro-targeting are sufficient enough to warrant an outright ban, as in *Sorrell,* there is a good argument that such a ban would be directed at the speaker (marketers) and content (advertising) that would almost surely be viewed as constitutionally impermissible. Instead, placing time, place or manner-type restrictions on the "speech" as would be the case with

discussed throughout this article. Finding how best to narrowly tailor the regulation to those interests, on the other hand, will be a significant challenge—a challenge Congress recently attempted.

Congress started to make some bipartisan movement over the past couple of years toward a more data-centric approach to national security and information harms. A 2019 bipartisan bill introduced in Congress requires big tech companies to start telling consumers about what data they are collecting, the value of that data, to obtain a consumer's "informed consent" before collecting data, and require companies to notify the public within 72 hours if a breach were to occur.[435] At the same time, Senators Elizabeth Warren, Lindsey Graham, and Amy Klobuchar introduced another bipartisan bill that would hold tech firms accountable for their role in protecting national security interests.[436] If such bills were enacted, the combined sum of the bills would help move the United States closer to addressing its core data problem and "reinforcing its defenses."[437]

These Congressional proposals are viable forward-looking solutions to the data problem, although only a first step. Giving consumers control over their data would do much to prevent abuses like Cambridge Analytica.[438] But this requires *real* control to be effective, which is to say that consumers should know where their data is headed and how it will be or could be used at the endpoint. Additionally, with the United States already amid a privacy revolution and being pushed in the direction of GDPR-like protections, the adoption of a national data protection regime seems to be a solution

additional consumer protections will likely pass scrutiny under a lower threshold. Ultimately, this is just one more reason why we have to regulate the underlying data collection and processing to decrease the amount of data flowing in the first place, before we even have to worry about corollary potential First Amendment protections.

[435] Grace Segers, *Senators Introduce Bipartisan Bill Forcing Tech Companies to Disclose Value of Users' Data*, CBS NEWS (June 25, 2019), https://www.cbsnews.com/news/senators-introduce-bipartisan-bill-forcing-tech-companies-to-disclose-value-of-users-data/; Shephard, *supra* note 368.

[436] *See* Rosenbach & Manstead, *supra* note 379.

[437] *Id.*

[438] Shephard, *supra* note 368.

in the right direction or at least one that might be inevitable anyway. Moving toward a national data protection regime is not too far from what was originally proposed in the initial stages of the U.S. Federal Privacy Act of 1974. In its original conception, the Federal Privacy Act required a purpose provision, included restrictions on onward transfers, and conditioned foreign transfers of information on either subject consent or equivalent protections abroad for the personal data.[439] While revisiting this legislation may serve as a good starting template for reform, the United States must be careful to enact something that puts citizens and civil liberties at the center while foreclosing data to adversaries.

Other bill proposals, like Senator Ron Wyden's recent "The Fourth Amendment Is Not For Sale Act," overlooks this "citizens at the center" approach, and could have far more implications for our national security than assumed.[440] "The Fourth Amendment Is Not For Sale Act" proposes to foreclose U.S. government agencies—specifically, intelligence and law enforcement agencies—from buying commercial data from third parties.[441] It may quell the public's concerns over ubiquitous commercial surveillance getting into the hands of the government. However, the bill does not address several foundational concerns, such as the overall core data broker business,

[439] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 911 (2009); *Legislative History*, Privacy Act of 1974, S. 3418, Pub. L. 93-579, 94th Cong. 7, 13-15 (1976).

[440] Katie Canales, *Sen. Ron Wyden is Introducing a Privacy Bill That Would Ban Government Agencies from Buying Personal Information From Data Brokers*, BUS. INSIDER (Aug. 4, 2020), https://www.businessinsider.com/ron-wyden-fourth-amendment-is-not-for-sale-privacy-2020-8; Steven Szymanski, *Is the Fourth Amendment Really for Sale? The Defense Intelligence Agency's Purchase of Commercially Available Data,* J. NAT'L SEC. L. & POL'Y (June 9, 2021), https://jnslp.com/2021/06/09/is-the-fourth-amendment-really-for-sale-the-defense-intelligence-agencys-purchase-of-commercially-available-data/#_edn20; *see* S. 1265, 117th Cong. (2021-2022) (Apr. 21, 2021). The "Fourth Amendment is Not for Sale Act" is described as "a bill to amend section 2702 of title 18, United States Code, to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, and for other purposes." *Id.* at Preamble.

[441] S. 1265, 117th Cong., § 2 (2021-2022) (introduced by Senate, Apr. 21, 2021).

the underlying algorithmic private surveillance practices now nearly shaping all Americans' internet experience, and the greater individual privacy issues or protection of rights.[442] Instead, "The Fourth Amendment Is Not For Sale Act" appears to address only a small subset of the issue involving the government purchase of commercially available data[443] and adopts a potentially flawed assumption about the privacy implications that flow from such transactions with the government.[444] Put in a different light, the bill looks toward the end of the data lifecycle to attempt to rectify harm rather than at the beginning (i.e., data creation versus data usage). Yet, when data is at the end of its lifecycle, it may be too late to guarantee fulsome protection from malicious actors or states, given the current U.S. privacy landscape.

An approach like Senator Wyden's "The Fourth Amendment Is Not For Sale Act" should cause considerable pause. The bill would foreclose the U.S. government, and specifically, those agencies charged with protecting against both physical and information harms, from having the same data and information that foreign governments and adversaries could likely obtain from data brokers or other entities in the business of buying and selling data (including those using advertising technology to create or elicit the data, similar to the approach used by Cambridge Analytica).[445] If the data can get in the hands of brokers or be commercially exchanged, it will inevitably get into the hands of foreign adversaries. This is the case even if other laws are in place to slow those transactions.[446] Thinking otherwise fails to

[442] *See generally id.*
[443] *Id.*
[444] *Cf.* Szymanski, *supra* note 440 (arguing that intelligence agencies actually have robust privacy protections and policy in place to protect the acquisition and use of commercially acquired data and that limiting this data to intelligence agencies would only hamper their national security mission).
[445] *See id.*
[446] *See* President Joseph R. Biden Jr., Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, WHITE HOUSE BRIEFING ROOM (June 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/; *Wyden Releases Draft Legislation to protect Americans'*

understand the information environment and digital age. For example, Cambridge Analytica, a company based in a U.S. partner nation, extracted and used commercial data, which ultimately facilitated adversarial foreign nation goals.[447] Senator Wyden's bill (and draft companion bill to address foreign transactions)[448] does not address this situation. The proposed bill, therefore, disadvantages U.S. agencies while adversaries or domestic, commercial, and criminal predators will continue to have access to the data. The bill may be a well-intentioned band-aid, but it will fail to alleviate a much deeper problem that stems from the underlying data practices themselves.

To address the gaps and concerns that the Wyden bill highlights, there must be a more holistic and foundational approach to controlling data access, not piecemeal and on the surface. The key to any data-centric approach to addressing information warfare and improving national security is foreclosing the data to everyone by limiting the creation of mass amounts of personal data in the first place; limiting personal data created to its initial intended, consensual purpose; preventing opaque data transfers to third parties who can launder the data away from it intended use; and by focusing on securing individual privacy through national privacy reform. Ultimately, the point of any new data protection regime should be to re-establish a healthy body politic that can become resilient to information harms, which tangentially secures the nation and our democracy.

V. NORMS

To round off a domestic analysis, it is important to address what influences domestic law on the fringes, both at home and abroad. A full domestic legal taxonomy of information warfare would not be

Personal Data From Hostile Foreign Governments, RON WYDEN U.S. SENATOR FOR OR. (Apr. 15, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments (providing draft legislation for comment to place safeguards for the sale of sensitive personal data to adversarial foreign governments).

[447] *See infra* Part IV. A.

[448] Wyden, *supra* note 446.

complete without at least minimally addressing how our domestic laws can influence and be influenced by norms. That is to say, international norm building is a means for the United States to indirectly control and protect access to people through the law.

At times in U.S. history, transnational movements have been essential to overcoming radical challenges to power and reconceptualizing constitutional limits.[449] Take for example the women's suffrage movement. At the time, U.S. constitutional law and political power dynamics prevented women from the right to vote.[450] American discourse surrounding the movement spurred an overwhelming international response that ended up supporting a transnational movement,[451] which served as the force to overcome seemingly impossible legal obstacles and political marginalization. The suffrage movement in the United States highlights that transnational support was required to cause such a radical change to power on the domestic front. With today's shifting power dynamics caused by the rise of the platform and surveillance economy and perceived constitutional bars to regulation, we cannot ignore the power of transnational movements to help move along the agenda to fight information warfare.

The first signs of international norms having a domestic impact are the appearance of those norms in domestic political discourse, changes in national institutions, and analysis of the state's policies.[452] Although the transnational legal process of compliance is a truly complex process of "institutional interaction whereby global

[449] *Cf.* Ellen Carol Dubois, *Woman Suffrage around the World: Three Phases of Suffragist Internationalism, in* SUFFRAGE AND BEYOND: INTERNATIONAL FEMINIST PERSPECTIVES 252-274 (Carline Delaney & Melanie Nolan, eds., 1994); Katherine M. Marino, *The International History of the US Suffrage Movement*, NAT'L PARK SERV. (last accessed May 17, 2020), https://www.nps.gov/articles/the-internationalist-history-of-the-us-suffrage-movement.htm#_ednref1.

[450] *See id.* ("A radical challenge to power, the U.S. movement for women's voting rights required transnational support to thrive").

[451] *See id.; Cf.* Dubois, *supra* note 409, at 254-255.

[452] Andrew P. Cortell & James W. Davis, Jr., *Understanding the Domestic Impact of International Norms: A Research Agenda*, 2 INT'L STUD. REV. 65, 69 (2000).

norms are not just debated and interpreted, but ultimately internalized by domestic legal systems,"[453] the United States can make initial steps in this direction by utilizing political discourse, changing national institutions, and reanalyzing state policies. As discussed in Part II, for example, transnational movements against information warfare targeting the anti-vaccination debate are well underway in Europe.[454] Surely, this is a movement the United States can join through political discourse, changes in national institutions, and analysis of policies. By embedding norms through these domestic mechanisms, the United States can show up for the information fight, albeit what might seem indirectly.

Pulling this thread further, today's information warfare is, in large part, caused by how Americans are changing *how* we as a nation and individuals speak to each other.[455] There is a very domestic "home-grown" element to information warfare that seems to be an insurmountable challenge to fix through our laws and policies. This is the other side of the information warfare fight, the one where America can only hope to lessen the harm.

The history of women's suffrage and its advancement through a transnational movement gives Americans insight into how to conceptualize fighting the homegrown information warfare harms today. During the twentieth century, suffrage activists benefited from international influence for the advancement of their U.S. domestic reform efforts when law and power at home seemed insurmountable to alter.[456] Additionally, women's suffrage is a history involving not only the right to vote but one that changed and advanced women's public speaking and the culture around that form of speech—[457] again, shifting *how* Americans once talked to each other.[458] Over time,

[453] Koh, *supra* note 312, at 2602.
[454] *See infra* Part II.C.
[455] *Cf.* Marantz, *supra* note 95, at 51-64.
[456] *See generally* Dubois, *supra* note 444; Marino, *supra* note 449.
[457] Judith Mattson Bean, *Gaining a Public Voice: A Historical Perspective on American Women's Public Speaking, in* SPEAKING OUT: THE FEMALE VOICE IN PUBLIC CONTEXTS 22, 27 (Judith Baxter ed., 2006).
[458] *See* Marantz, *supra* note 95, at 51-64.

traditions and ideals regarding woman's public speech were shaped through changing cultural norms, undoubtedly shaped by those transnational movements.[459]

Judith Mattson Bean, a scholar who studied the history of woman's speech noted, "[a] particular culture or speech community determines who that community will accept as a public speaker, not usually by law but by customs that are linked with that culture's norms of leadership, power, and range of speech events."[460] Although law may not be a direct mechanism to alter culture, it most certainly can do so indirectly. Law has the power to alter those acceptable norms of leadership, power, and speech events. Reform to domestic laws can rearrange leadership and power through designations of critical infrastructure, reducing the effects of the unequal power dynamics between private platforms and government. Laws can also change the power dynamics by allowing individuals to regain control and power over their data and minimizing the data available for profits and abuse. Finally, law can be reconceptualized to define a permissible scope of speech events that mitigate information harms, such as how content is provided to individuals by reducing the effects of microtargeting or amplification.

From the government to the general public, America must work toward building and maintaining those legal and normative mechanisms that foster transnational movements to change how we as a nation speak to each other, a state of affairs that has dramatically altered since the rise of the information platform economy. Only at that point might the nation be able to address some of the most challenging foreign and homegrown domestic information harms caused merely by pure sport, hobby, or newly developed monetary ventures at home.[461] If our speech community is now a global community,[462] then global norms and customs must be sought to

[459] *Cf. generally* Bean, *supra* note 457; Marino, *supra* note 449.
[460] Bean, *supra* note 457, at 22.
[461] *See* Marantz, *supra* note 95, at 51-64; *Cambridge Analytica and the Future of Data Privacy, supra* note 107, at 7 (written statement of Eitan Hersh,).
[462] See *supra* discussion in part III.A.2; *see also* Packingham v. North Carolina, 137 S. Ct. 1730, 2732 (2017).

shape who will be accepted as a public speaker.[463] The hope is that these norms and customs will develop to crowd out and reject those that espouse and cause information harm. This hope, however, can only become a reality if the United States starts adding to the discourse of those global norms and customs, which starts with our domestic laws at home.

The importance of this domestic and international interaction today cannot be overstated. We are in the midst of witnessing the effects that international laws have on our own U.S. domestic legal system. The GDPR, discussed in Part IV, prompted "a tidal wave of public support for a privacy law revolution" in America. The GDPR now serves as a quintessential example of a domestic law having global effects and causing its own transnational movement today. The United States needs to be a part of that movement, otherwise, it risks having its interests overcome by other international actors and losing the opportunity to shape the quickly evolving laws and norms surrounding information harms.

More importantly, when U.S. laws fail to provide adequate protections—a situation that the United States may find itself in more times than not when addressing its ability to combat information warfare—it will need to look to the international community for legal gap fillers and outside influence. The vital role played by the international community in this space is already evident when looking at how international pressure addressed information warfare campaigns targeting health disinformation. The United Kingdom and other countries passed laws and placed pressure on international social media platforms to change their algorithms and cut out anti-vaccination disinformation,[464] including some moves that the First Amendment might sound the death knell for if attempted in the United States. Americans still get to benefit from these platform changes caused by this international influence due to the global nature of the platform economy.

---

[463] *Cf.* Bean, *supra* note 457, at 22.

[464] *See* Corn, *supra* note 125.

Understanding the importance of international norm building and transnational movements and how the development of domestic law can foster these mechanisms is, therefore, a key component in our arsenal of tools for combating information warfare. While it may be an indirect tool, it nonetheless may be the most effective.

VI. CONCLUSION

Defining and understanding a problem is essential to addressing a problem; any operational planner preparing for a fight knows this maxim.[465] If the problem of information warfare requires a whole-of-society approach, then all of society needs a common definition to address this problem. A common definition helps identify and isolate the root causes of the problem.[466] Failing to identify all root causes may lead decision-makers to misunderstand the full scope of the problem and to overlook all viable avenues of approach. Within the legal context, this may even lead many to believe that U.S. laws and policies leave Americans helpless to the harms of information warfare, or worse yet, require the loss of civil liberties.

To fill this potentially dangerous gap, this article proposed a common definition that helps identify and isolate root causes. While there likely can never be a perfect or absolute definition for this enormous and deeply complex problem, a definition that can at least begin to bring Americans together under a unified understanding is one that defines information warfare as *maliciously accessing people in the information environment, intending to manipulate or disrupt, for political ends*. The definition informs society that information warfare is about gaining access, controlling access, and abusing power from such access.

By adopting this broadly scoped definition to inform the American national consciousness, a wide net can be cast to better understand the root causes of the problem. These causes of content,

[465] *See* Joint Publication, 5-0, Joint Planning IV-14 (2017).
[466] *Cf. id.*

data, and norms can be better understood as the main avenues for attack for accessing people within the information environment. Directing attention to these vectors of attack from a domestic standpoint gives us a viable path toward understanding how to fight back against information warfare through the law. In the end, to fortify the U.S. homeland from information warfare, America must not tie its hands by only looking at the content. America must think about what is behind that content by looking at the overall malicious activity and underlying data, as well as by looking beyond its borders. It is far more than just fighting words.