

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

TIKTOK INC. and BYTEDANCE LTD.,

Plaintiffs,

v.

Civil Case No. 20-cv-2658

DONALD J. TRUMP, in his official capacity as President of the United States; WILBUR L. ROSS, JR., in his official capacity as Secretary of Commerce; and U.S. DEPARTMENT OF COMMERCE,

Defendants.

DECLARATION OF PROFESSOR STEVEN WEBER

I, Steven Weber, under penalty of perjury, hereby declare as follows:

1. I am Professor and Associate Dean of the School of Information, and Professor of Political Science, at the University of California, Berkeley. I am also the founder and faculty director of the Center for Long Term Cybersecurity at UC Berkeley, where I lead a multi-disciplinary research group that works on emerging digital security issues at the intersection of new technologies, human behavior, and risk calculations made by firms and governments. I received a Ph.D. in political science at Stanford University in 1989 and have been a professor at Berkeley since 1989. I have attached a true and complete copy of my curriculum vitae to this declaration.

2. I focus upon U.S. national security issues with particular expertise in how digital technologies impact and are impacted by national and international security. I have written three relevant university press peer-reviewed books and a number of peer-reviewed journal articles on this subject, as well as many other articles for non-peer reviewed publications. I have served as a

consultant to a wide variety of U.S. and global firms as well as U.S. government agencies dealing with strategic issues at the intersection of national security and the digital economy.

3. I have been retained by the plaintiffs in this case to analyze the stated justifications of President Trump’s Executive Order of August 6, 2020 relating to the TikTok software application (“the August 6 order”), which are incorporated by reference in the Department of Commerce action issued on September 20, 2020.¹ As I discuss below in greater detail, these justifications center on two issues: (1) the security of the data that TikTok collects from its users, particularly as it relates to possible disclosure to the Chinese government; and (2) the possibility that the TikTok recommendation algorithm (i.e., the computer code that selects what videos to present in a user’s feed) could be misused for the benefit of the Chinese government, either by censoring content or for affirmative propaganda or disinformation campaigns.²

4. As I discuss below, these issues are not unique or even distinctive to TikTok. It is inherent in digital technologies that every company, governmental entity, and non-governmental organization faces risks to the security of the data it stores—whether on behalf of employees,

¹ The Department of Commerce action, which is entitled “Identification of prohibited transactions,” does not elaborate upon or add new justifications to the stated justifications provided by President Trump in his August 6 order.

² The order states that: “These risks are real. The Department of Homeland Security, Transportation Security Administration, and the United States Armed Forces have already banned the use of TikTok on Federal Government phones. The Government of India recently banned the use of TikTok and other Chinese mobile applications throughout the country; in a statement, India’s Ministry of Electronics and Information Technology asserted that they were ‘stealing and surreptitiously transmitting users’ data in an unauthorized manner to servers which have locations outside India.’ American companies and organizations have begun banning TikTok on their devices.” I note that this statement refers to steps taken by various organizations to respond to their *perception* of threat posed by TikTok, and is not an independent justification for the steps taken in the order.

customers, or others.³ Such major U.S. companies as Yahoo, Target, Equifax, eBay, LinkedIn and many others have suffered well-known breaches of millions of user records.⁴ As for the asserted issues pertaining to TikTok’s algorithm—which are better understood as assertions pertaining to ‘algorithmic integrity’—those are likewise issues that the social media and many other industries are dealing with more generally and have been for years. For example, YouTube has added disclaimers to certain channels that are reportedly being used to spread disinformation on behalf of the Russian government.⁵

5. Before turning to these specific issues, there are two general information security principles that should be kept in mind. First, data security is not a binary switch that can be toggled on or off. There are always tradeoffs being made among the three core components of security: confidentiality, integrity, and availability of data.⁶ As with many enterprise risks, data security is an exercise in risk management—identifying risks, assessing them, and mitigating those risks to acceptable levels at an appropriate cost.⁷ Second, when it comes to data security threats, it is

³ See, e.g., U.S. Department of Homeland Security, *Cybersecurity Strategy* (May 15, 2018).

⁴ See the summary review of recent large data breaches in Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO Online, (April 17, 2020), at <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

⁵ Paresh Dave, *Russian disinformation on YouTube draws ads, lacks warning labels: researchers*, Reuters (June 7, 2019), at <https://www.reuters.com/article/us-alphabet-google-youtube-russia/russian-disinformation-on-youtube-draws-ads-lacks-warning-labels-researchers-idUSKCN1T80JP>.

⁶ This ‘CIA’ triad is carefully explained by NIST in *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, at <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.

⁷ See, e.g., U.S. Department of Homeland Security, *Cybersecurity Strategy*; National Institute of Standards and Technology, *Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations 12* (April 2013).

virtually impossible to prove the negative and establish that there are *no* risks to a particular network or data storage and management system.⁸ Sophisticated organizations and information security professionals understand that malicious actors are constantly evolving, which means the threat landscape is always changing. Even an organization that maintains best-in-class security practices across the board cannot with full confidence assert that there is no risk that its data could be inadvertently accessed or disclosed. These principles form the basis of the most sophisticated data security programs and strategies in the most advanced organizations.

6. With the foregoing as background, I address the two issues cited as justifications for the August 6 order: data security and algorithmic integrity.

I. Data Security

7. The first stated basis for the August 6 order is that: “TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.”

8. As an initial matter, the assertion that TikTok “captures vast swaths of information from its users” is principally a statement about data privacy, not data security. There is a separate policy debate about the extent to which social media and other digital product companies collect information from users, and this debate is beyond the scope of my testimony. The August 6 order does not maintain that TikTok’s data collection practices are themselves the basis for the order,

⁸ Shuman Ghosemajumder, *You Can’t Secure 100% of Your Data 100% of the Time*, Harvard Business Review (Dec. 4, 2017), at <https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time>.

except insofar as this collection “threatens to allow the Chinese Communist Party” access to the data that has been collected. This *is* an assertion about a data security risk because it is an issue of who has access to data and for what purpose. I focus on principles of data security in analyzing this aspect of the order.

9. As security professionals in industry and regulators have responded to the threats of data breaches and other threats to data security, they have increasingly coalesced around a set of best practices for mitigating data security risk.⁹ A comprehensive overview of these data security best practices is beyond the scope of this testimony but there are a few important standards around security controls that are particularly relevant to the concerns expressed in the August 6 order. First, it is preferable from a data security perspective to segment and tightly control access to a company’s sensitive data, such as TikTok’s U.S. user data in this case, and to maintain and audit access logs so that any deviations from expected behaviors, including unauthorized access, can be identified and addressed.¹⁰ Second, sensitive user data should be stored in encrypted form using industry-standard methods, rather than unencrypted form. This is essential because if stored data (‘at rest’) should somehow be the subject of an unauthorized access, it will be indecipherable to and unusable by persons or organizations who lack an encryption key.¹¹ Similarly, when data is being transmitted across the Internet, it is equally important from a data security standpoint to

⁹ See Federal Trade Commission, *Start with Security* (June 2015); Thomas B. Pahl, *Stick with Security: Segment your network and monitor who’s trying to get in and out* (Aug. 25, 2017), at <https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-segment-your-network-monitor-whos-trying-get>; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018).

¹⁰ See for example CISCO’s *A Framework to Protect Data Through Segmentation* at https://tools.cisco.com/security/center/resources/framework_segmentation.

¹¹ See for example Microsoft’s *Azure Data Encryption at Rest* (Aug. 13 2020), at <https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest>.

encrypt the data ‘in motion’—this similarly will prevent any malicious actor who is able to intercept the data in transmission from using it in any meaningful way.¹² Third, the encryption keys themselves must be secure from unauthorized access, and companies should have robust review processes for assessing legitimate business need to access data at any time in decrypted form.¹³

10. I have reviewed the declaration of Roland Cloutier, TikTok’s Chief Security Officer, and have also reviewed other data security-related materials the company has made public. At a high level, TikTok’s approach to data security is in line with other sophisticated technology companies that employ industry best practices. In particular and with respect to the most important practices discussed above, I note that TikTok has segmented U.S. user data, and has imposed access control and auditing policies that limit and track access to customer data. TikTok encrypts user data in storage and during transmission using industry-standard Key Management Service algorithms. TikTok’s U.S.-based security team manages the keys that are needed to decrypt the data for legitimate purposes. ByteDance personnel cannot access these data except through a formal approval process that requires documented and demonstrated need and is subject to approval by the U.S.-based security team, on a least-privilege basis (meaning that approval is granted for the lowest level of access sufficient for the requested work). These controls are consistent with industry best practice.

11. I note also that these controls are particularly responsive to the asserted basis for

¹² See for example Avast Security’s *Data in Transit Encryption* (April 25, 2020), at <https://securityboulevard.com/2020/04/data-in-transit-encryption-avast/>.

¹³ See for example NIST’s *Cryptographic Key Management: What are Best Practices for Organizations?* (April 11, 2018), at <https://csrc.nist.gov/News/2018/NIST-releases-Draft-SP-800-57-Part-2-Rev-1>.

the August 6 order, since they mitigate the risk of an ‘insider’ associated with the Chinese government accessing and disclosing U.S. customer data to the Chinese government. (Of course, the hypothetical risk that an engineer might seek to disclose user data to the Chinese government is not limited to companies that are *owned* by Chinese nationals or *headquartered* in China. Many multinationals have extensive software and other engineering operations in China, for example, which would present effectively the same risk.)

II. Algorithm Security

12. The second stated justification for the August 6 order pertains to the recommendation algorithm. The order states: “TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China’s treatment of Uyghurs and other Muslim minorities. This mobile application may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus.”

13. The term ‘censorship’ has a pejorative connotation, but content moderation and algorithmic curation in online platforms are not *prima facie* equivalent to censorship. The issue around censorship is whether an algorithm of this kind can be used to manipulate opinions or change perspectives in illegitimate ways. Here again, this is an industry-wide issue and not an issue limited to TikTok. The same concerns apply to a wide range of digital media providers, such as Facebook, Instagram, Apple News, and essentially all digital content providers. Twitter attempts to block violence-promoting tweets.¹⁴ Facebook has an evolving set of policies that

¹⁴ <https://help.twitter.com/en/rules-and-policies/twitter-rules>.

attempt to block various kinds of hate speech.¹⁵ YouTube has modified its content promotion policies in an attempt to reduce radicalization and the firm reports, for example, that it removed over 11 million videos from the site in the 3 month period spanning April to June 2020.¹⁶

14. From a national security perspective, the question is whether the algorithm is legitimately shaping the flow of content in accordance with a commercial product strategy, along with appropriate restrictions to counter illegal or otherwise proscribed activity (such as hate speech) consistent with public terms of use. Or is the algorithm illegitimately seeking to manipulate users' perspectives and opinions in directions that serve a foreign states' short and long term strategic interests at odds with those of the United States. Specifically with regard to TikTok, that resolves into the following question: does there exist evidence and reason to believe that TikTok is now or would become essentially an algorithmic propaganda tool of the Chinese government or Chinese communist party?

15. Based on the information I have reviewed, my conclusion to this question is "no." The starting point for this assessment is that a small number of anecdotes about 'censored' or 'promoted' content (such as those cited in the August 6 order) do not in and of themselves demonstrate a national security risk. That is partly because algorithmic content moderation and user experience customization is based on a fast-evolving science that involves state-of-the-art machine learning techniques to solve some of the hardest problems in image recognition, natural language processing, and other related areas that sometimes go under the label of 'Artificial Intelligence'. Like humans, algorithms make mistakes and learn from those mistakes (thus the term 'machine learning' is a more accurate and useful descriptor than is 'artificial intelligence').

¹⁵ <https://www.facebook.com/communitystandards/>.

¹⁶ <https://transparencyreport.google.com/youtube-policy/removals?hl=en>.

In most firms, algorithmic moderation is supplemented by human content moderators who typically make assessments about ‘gray’ or uncertain cases where algorithmic decision making is ambiguous, as well as overseeing how algorithms perform relative to the platforms’ strategy. The question, accordingly, is whether social media platforms react and evolve as they develop their technologies and practices over time and in response to concerns, complaints, and errors.

16. An example of this evolutionary process can be seen in public reports of how ByteDance responded to allegations that its news aggregator app in Indonesia (known locally as Baca Berita or BaBe) was in 2018 removing articles that could be construed as critical of the Chinese government.¹⁷ BaBe was purchased by ByteDance in 2018 after TikTok, which had experienced explosive growth among young Indonesians very much like it has inside the United States, was temporarily banned in Indonesia for ‘inappropriate content’ including pornography. As part of ByteDance’s efforts to persuade the Indonesian government to reverse the ban, an agreement was reached to hire a team of local moderators for TikTok. Around the same time, a source reported that local content moderation practices at BaBe were being inappropriately influenced by a team from ByteDance’s offices in Beijing, while BaBe maintained that it moderated content according to its local terms of service and Indonesian law. ByteDance and BaBe report different dates around which these practices changed, but what is clear is that by mid-2020 articles on previously restricted topics that formed the basis of the censorship accusation were available to read on the platform. This example is relevant because it bears directly on the processes by which content moderation (both algorithmic and human) evolves and provides a

¹⁷ Fanny Potkin, *Exclusive: ByteDance Censored Anti-China Content in Indonesia Until Mid-2020*, *Sources Say*, Reuters Business News (Aug. 13, 2020), at <https://www.reuters.com/article/us-usa-tiktok-indonesia-exclusive/exclusive-bytedance-censored-anti-china-content-in-indonesia-until-mid-2020-sources-say-idUSKCN2591ML>.

template against which to assess what is being done and proposed for TikTok’s U.S. operations.

17. In other words, algorithms must be understood in conjunction with companies’ overall strategic choices about content curation and with human content moderation teams that are called on to deal with ambiguous or particularly complicated cases. TikTok’s content moderation for U.S. users, importantly, is led by a team in the United States. Going further, TikTok in late July 2020 announced the creation of a ‘Transparency and Accountability Center’ where outside experts and researchers will have the opportunity to “observe our moderation policies in real-time, as well as examine the actual code that drives our algorithms.”¹⁸ This is a very positive move and is unprecedented for technology or social media companies. In my view TikTok here sets a new ‘gold standard’ that other social media companies will be pressured to meet, to the overall good of the industry.

III. Conclusion


18. Social media platforms like TikTok raise important policy issues, including the appropriate protection of user data, content moderation, and disinformation. These are legitimate issues to consider from a policy perspective, but they are issues that the industry confronts as a whole and are not unique or distinctive to TikTok. As I have discussed above, TikTok’s approach for dealing with these issues is generally in line with—and in some respects markedly better than—industry best practices, even for companies that hold significant sensitive user data. In light of the foregoing, there is no evident national security rationale for banning TikTok, as the August 6 order has directed. It is arbitrary to select one market participant and ban that particular firm for policy issues that an entire industry faces. This is particularly the case where there exists alternative

¹⁸ Kevin Mayer, *Fair Competition and Transparency Benefits Us All*, TikTok blog (July 29, 2020), at <https://newsroom.tiktok.com/en-us/fair-competition-and-transparency-benefits-us-all>.

mechanisms—the mitigation proposals made in the CFIUS process—that enable U.S. government agencies to mitigate national security risks around data and algorithms *beyond* what they would be currently be able to achieve with competitor firms.

Pursuant to 28 U.S.C. § 1746 and under penalty of perjury, I affirm that the foregoing facts are true and correct to the best of my knowledge.

Executed this 21st day of September, 2020.



Steven Weber

STEVEN WEBER

Professor, School of Information and Department of Political Science
Associate Dean, School of Information, Division of Computing, Data Science, and Society
Director, Center for Long Term Cybersecurity
UC Berkeley School of Information
203 B South Hall
UC Berkeley, Berkeley CA 94720

Tel 415/203.8432 (Mobile) 510/643.3755 (Office)
steve_weber@berkeley.edu

Major Fields of Work

International Relations Theory, particularly theories about cooperation and competitiveness
International Institutions
Political Economy of Networks/Internet
European Union Politics
American Foreign Policy, particularly National Security and FDI Issues
Applications of Cognitive and Behavioral Psychology to Decision-making Research
Scenarios and Strategic Planning

Education

July 1988 June 1989 Postdoctoral Fellow Center for International Affairs, Harvard University
March 1985 June 1988 Ph.D., Stanford Dept. of Political Science
Sept. 1982 June 87 M.D. Student, Stanford Medical School
Sept 1984 March 85 M.A. Stanford Dept. of Political Science
Sept 1979 June 82 B.A. Washington University (History, International Development)

Major External Grants and Fellowships

Summer 2017: MacArthur Foundation, Protecting Vulnerable Individuals Online
Winter 2016: Hewlett Foundation, Privacy and Internet of Things
Winter 2015: Hewlett Foundation, Center for Long Term Cybersecurity
Winter 2012: Kaufmann Foundation, Political Economy of Shared Data
Fall 2007: Energy Biosciences Institute Principal Investigator
Winter 2005: Carnegie Corporation and Rockefeller Brothers Fund Grants for New Era Foreign Policy Project (Carnegie renewed in 2008, 2011, 2013, 2015, 2018)
Winter 2004: NSF, Information Technology for Billions (IT4B)
Spring 2003: SITRA Grant, Research in Open Innovation Networks
Winter 2002: Ford Foundation Grant, Scholar in Information Technology and International Relations
June 2001: Senior Advisor, Policy for A Networked Society, The Markle Foundation, NY.

April 2001: Industry-University Consortium Research Policy Grant for Open Source Software Research

June 2001: European Union Center Grant

January 1995: MacArthur Foundation program in Multilateral Institutions in World Politics at Berkeley (3 year renewal).

1995-96: Fellow at Center for Advanced Studies in Behavioral Sciences, Stanford CA

January 1992: Simpson Chair in International Studies at University of California, Berkeley.

June 1991: Council on Foreign Relations, International Affairs Fellowship (term: Calendar Year 1992) Position: Political Consultant to the President, European Bank for Reconstruction and Development, London.

June 1989: Helen Dwight Reid Award of American Political Science Association, Best Dissertation in International Relations

July 1987: "New Faces" in International Security Conference, IISS and Rockefeller Foundation, Bellagio, Italy.

April 1987: Arms Control Fellow (Predoctoral), Stanford Center for International Security and Arms Control

Jan. 1986: U.S. Department of Education, National Graduate Fellow in Political Science

Nov. 1985: MacArthur Fellow in International Security Studies, Stanford

Administrative Appointments

Director, Institute of International Studies, UC Berkeley. 2004-2009

Director, Center for Long Term Cybersecurity, UC Berkeley, 2015 - ongoing

Associate Dean, I School and CDSS, 2020-ongoing

Major Publications

Books

Bloc By Bloc: How to Organize a Global Enterprise Harvard University Press, 2019

The End of Arrogance: America in the Global Competition of Ideas Harvard University Press, 2010 (with Bruce Jentleson)

The Success of Open Source Harvard University Press, 2004.

Cooperation and Discord in US-Soviet Arms Control, Princeton University Press, 1991.

Edited Books

Deviant Globalization: Black Market Economy in the 21st Century Continuum Press, 2011 (with Nils Gilman and Jesse Goldhammer)

Globalization and The European Political Economy Columbia University Press, 2001.

European Integration and American Federalism: A Comparative Perspective (with Richard Herr). Berkeley: University of California, International and Area Studies, 1996.

Monographs

Shaping the Postwar Balance of Power 1947/1961: Multilateralism in NATO, UC Berkeley Institute of International Studies, Research Papers in International Affairs, Spring 1991. A shorter version of this monograph appears as a chapter in Multilateralism Matters: The Anatomy of an Institution, edited by John Ruggie, Columbia University Press, 1993.

Cybersecurity Futures 2020. Report issued by the Center for Long Term Cybersecurity UC Berkeley 2015

Coauthored Books

Tracking A Transformation (with BRIE co-authors). Brookings Institution Press, 2001.

The Highest Stakes: Economic Foundations of the New Security Order, Oxford University Press, 1992. (with John Zysman, Micheal Borrus, et. al.

Selected Papers

"Realism, Detente, and Nuclear Weapons", International Organization 44. Winter 1990.

"Cooperation and Interdependence", Daedalus, 120, Winter 1991. [Reprinted in Emannuel Adler, ed., The Theory and Practice of Arms Control, Johns Hopkins University Press, 1992.]

Origins of the European Bank for Reconstruction and Development. Working Paper Series, Harvard University Center for European Studies, 1992.

"Shaping the Postwar Balance of Power", International Organization 46. Summer 1992.

"Mercantilism and Global Security" (with John Zysman and Michael Borrus), The National Interest, Autumn 1992.

"Origins of the European Bank for Reconstruction and Development", International Organization 48. Winter 1994.

"International Political Economy 'After' The Business Cycle". Journal of Social, Political, and Economic Studies. 21. Fall 1996.

"The Changing Politics of EMU", Swiss Political Science Review. 2. Fall 1996.

"The End of the Business Cycle?" Foreign Affairs July-August 1997.

"Prediction and the Middle East Peace Process", Security Studies 6. Summer 1997.

"Emerging Markets: Good for US? Good for Everyone?" (with Elliot Posner), Brown Journal of International Affairs. Summer 1998.

"Five Scenarios of the Israeli-Palestinian Relationship in 2002," Security Studies 7. Summer 1998 (with Janice Stein et.al.)

"Organizing International Politics: Sovereignty and Open Systems," (with Christopher Ansell) International Political Science Review. January 1999.

"A Certain Idea of Nuclear Weapons: France's Non-Proliferation Policies in Theoretical Perspective," (with Nicolas Jabko), Security Studies 8. Winter 1999.

"God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World," European Journal of International Relations 6. Winter 2000. (with Janice Stein, Ned Lebow, and Steven Bernstein)

"International Organizations and the Pursuit of Justice in the World Economy," Ethics and International Affairs, Winter, 2000.

"Creating a Pan-European Equity Market: The Origins of EASDAQ," Review of International Political Economy Winter 2001 (with Elliot Posner)

"The Political Economy of Open Source Software" BRIE Working Paper # 140, University of California, Berkeley. At <http://brie.berkeley.edu/~briewww/pubs/wp/wp140.pdf> (A shorter version is published in Tracking a Transformation, Brookings Institution, 2001).

"E-Finance and the Politics of Transitions," in "Electronic Finance: A New Perspective and Challenges," BIS Paper No. 7 (Bank of International Settlements, November 2001). (with John Zysman)

"The New Economy and Economic Growth in Developing Countries: Speculations on the Meaning of Information Technology for Emerging Markets", (with John Zysman). Emergo: A Journal of Transforming Economies and Societies, 2003.

"Will Information Technology Reshape the North-South Asymmetry of Power in the Global Political Economy?" (with Jennifer Bussell). Studies in Comparative International Development 40. Summer, 2005.

"Getting to No," (with James Goldgeier), The National Interest, Winter 2006.

“The International Implications of China’s Fledgling Regulatory State: From Product Maker to Rule Maker” (with Abraham Newman and David Bach), New Political Economy December 2006.

“How Globalization Went Bad” (with Naazneen Barma, Ely Ratner, and Matthew Kroenig), Foreign Policy 2007.

“A World Without the West,” (with Naazneen Barma and Ely Ratner), The National Interest. 2007.

"America's Hard Sell," (with Bruce Jentleson), Foreign Policy 2008.

“A World Without the West: Empirical Patterns and Theoretical Implications,” Chinese Journal of International Politics 2, 2009. (with Naazneen Barma, Giacomo Chiozza, and Ely Ratner)

“Taking Soft Power Seriously,” Comparative Strategy 2010 (with Matthew Kroenig and Melissa McAdam)

“The Mythical Liberal Order”, The National Interest 2013 (with Naazneen Barma and Ely Ratner)

‘Visualizing ambivalence: showing what mixed feelings look like’. (with Galen Panger and Bryan Rea) 2013. In CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13). ACM

‘Back in the USSR: Is the European Union Heading for a Soviet-Style Collapse?’ The American Interest (with Nils Gilman) December 2016

“The New World of Data: Four Provocations on the Internet of Things” (with Richmond Wong), First Monday February 2017.

“Can You Secure an Iron Cage?” (with Nils Gilman and Jesse Goldhammer), Limn 8 2017.

‘Coercion in Cybersecurity: What Public Health Models Reveal’, Journal of Cybersecurity May 2017

‘Data, Development, and Growth,’ Business and Politics September 2017

“Moving Slowly, Not Breaking Enough: Trump’s Cybersecurity Accomplishments” (with Betsy Cooper), Bulletin of the Atomic Scientists October 2017.

‘The Long Game of Chinese Techno-nationalism’, (with Shazeda Ahmed), First Monday April 2018.

Selected Book Chapters etc

"U.S. Soviet Attempts to Regulate Military Activities in Space", in U.S. Soviet Security Cooperation: Achievements, Failures, Lessons. Alexander George, Phillip Farley, Alexander Dallin, editors. Oxford University Press, 1988. (with Sidney Drell)

"Interactive Learning in US Soviet Arms Control", in Learning in US and Soviet Foreign Policy, George Breslauer and Philip Tetlock, eds., Westview Press, 1991.

"The Superpowers and Regional Conflicts After the Cold War", in Breslauer, Kriesler, and Ward, ed. Regional Conflicts after the Cold War, Institute of International Studies, Berkeley, 1991.

"Does NATO Have A Future?", Beverly Crawford, ed. The Future of European Security, IIS, Berkeley, 1992.

"Security After 1989," in Nuclear Weapons In The Changing World : Perspectives From Europe, Asia, and North America, Patrick Garrity and Steven A. Maarenan eds. New York: Plenum Press, 1992.

"Institutions and Change", in Micheal Doyle and G. John Ikenberry, eds. New Thinking in International Relations, Westview Press, 1997.

"European Union Conditionality", in Barry Eichengreen, Jeffrey Frieden, and Jurgen Von Hagen, eds. Politics and Institutions in an Integrated Europe, Springer-Verlag, Berlin, 1995.

"Counterfactuals Past and Future", in Phillip Tetlock and Aaron Belkin, eds., Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives, Princeton University Press, 1996.

"Nested Institutions and European Monetary Union", in Vinod Aggarwal, ed. Institutional Designs for a Complex World : Bargaining, Linkages, and Nesting Cornell University Press, 1998.

"Why the Changed Relation Between Security and Economics Will Alter the Character of the European Union", (with John Zysman), in Zysman and Andrew Schwartz, eds., Enlarging Europe: The Industrial Foundations of a New Political Reality Berkeley: IAS, 1998.

"A Modest Proposal for NATO Expansion", in Robert W. Rauchhaus (ed.), Explaining NATO Enlargement, London: Frank Cass, 2000. Also in Contemporary Security Policy, Vol.21, No.2 August 2000.

"Governance and Politics of the Internet Economy -- Historical Transformation or Ordinary Politics With a New Vocabulary?" (with John Zysman) in International Encyclopedia of the Social and Behavioral Sciences, Neil Smelser and P. B. Baltes, eds. Oxford: Elsevier, 2000.

"National Security and The War Potential of Nations," in International Encyclopedia of the Social and Behavioral Sciences, Neil Smelser and P. B. Baltes, eds. Oxford: Elsevier, 2000.

"Tools for Thought", in Tracking a Transformation, Brookings Institution, 2001. (with Brad DeLong, John Zysman, and Stephen Cohen).

"The Political Economy of Open Source Software and Why It Matters," in Digital Formations: IT and New Architectures in the Global Realm, Robert Latham and Saskia Sassen, eds. New Jersey: Princeton University Press, 2005.

"Patterns of Governance in Open Source," in Chris DiBona, Danese Cooper, and Mark Stone, eds., Open Sources 2.0, The Continuing Evolution. Sebastopol CA: O'Reilly, 2005.

"From Linux to Lipitor: Pharma and the Coming Reconfiguration of Intellectual Property," in John Zysman and Abraham Newman, eds., How Revolutionary was the Digital Revolution: National Responses, Market Transitions, and Global Technology. Stanford CA: Stanford University Press, 2006.

"Probing the Value of Shared Data in the Modern Economy", Report to the Kaufmann Foundation, 2012 (With AnnaLee Saxenian)

"Deviant Globalization," (in Michael Miklaucic and Jacqueline Brewer, ed., Convergence: Illicit Networks and National Security in the Age of Globalization, National Defense University Press, 2013 (with Nils Gilman and Jesse Goldhammer)

"Why Universities and Foundations Should Get Together Sooner", Chronicle of Higher Education April 2017 (with James Goldgeier, Bruce Jentleson, and Jessica Trisko Darden.)