Texas A&M Law Review

Volume 2 | Issue 4

Article 3

2015

Introduction to the Symposium Edition: New Technology and Old Law: Rethinking National Security

Lisa A. Rich
larich@law.tamu.edu

NATIONAL SECURITY SYMPOSIUM

INTRODUCTION TO THE SYMPOSIUM EDITION: NEW TECHNOLOGY AND OLD LAW: RETHINKING NATIONAL SECURITY

By: Lisa A. Rich

TABLE OF CONTENTS

This special Symposium Edition of the *Texas A&M Law Review* contains selected articles from presenters at the Fall Symposium entitled *New Technology and Old Law: Rethinking National Security* held at the Texas A&M School of Law on October 17, 2014. The symposium brought together some of the country's leading scholars and practitioners on issues related to national security. Symposium participants specifically examined the challenges presented to existing domestic and international-legal frameworks to adapt to emerging national security threats. Panelists provided critical analysis of major issues including the use of Unmanned Aerial Vehicles (UAVs)/drones, big data and mass surveillance, cyber security and issues of privacy, the growth of asymmetric warfare, and challenges from new coalitions such as ISIS/ISIL.

I. INTRODUCTION

The term national security is one that means many things to many people, whether policymakers or average citizens,[1] despite the fact

[1] *See* Arnold Wolfers, *National Security as an Ambiguous Symbol*, 57 POL. SCI. Q. 481 (1952).

that the "term national security . . . is well enough established in the political discourse of international relations."[2] In its most broad and somewhat simplistic sense, "national security" is a collective term encompassing both national defense and foreign relations in the United States. Specifically, as some have defined it, national security is the condition provided by (1) military or defense advantage over any foreign nation or group of nations; (2) favorable foreign relations position; or (3) defense posture capable of successfully resisting hostile or destructive action from within or without—whether overt or covert.[3] Thus, a nation is "secure" when it is "not in danger of having to sacrifice its core values, if it wishes to avoid war, and is able, if challenged, to maintain" those values through use of force.[4] None of these definitions, debated vigorously throughout United States history, are completely on point, yet they help frame the general discussion that occurred during the Symposium and which is further developed in this edition.

As we solidly enter the 21st century—in which every day seems to bring news of some significant potential threat to our national security—policymakers, stakeholders, and we as citizens are being asked to re-examine our legal, social, economic, and military structures to determine whether they are sufficient to meet the goals, challenges, and ideals of the coming months, years, and decades. And, as part of those examinations, we are examining our core values and asking how they influence our national security.

In this era of modernity, every day not only brings exciting advances in technology, science, and human understanding, but also news of collective threats—be they foreign or domestic, natural or manmade, that challenge our "national security." These events not only seem prolific but seem to challenge our very foundations of government and defense with such speed that at times we seem almost incapable of responding or adapting despite the virtual explosion of access to information and intelligence that has occurred over the past two decades. As Dr. Henry A. Kissinger stated before the Senate Armed Services Committee, "The United States has not faced a more diverse and complex array of crises since the end of the Second World War."[5] Secretary Madeleine K. Albright echoed these observations, "It does not take a seasoned observer of international relations to

[2] *Id.* at 483.

[3] William M. Arkin et al., Encyclopedia of the U.S. Military 444 (1990).

[4] Wolfers, *supra* note 1, at 484 (citing Walter Lippmann, U.S. Foreign Policy: Shield of the Republic 51 (1943)).

[5] *Global Challenges and the U.S. National Security Strategy Before the Senate Armed Services Committee*, 114th Cong. 5, at 31 (2015), http://www.armed-services.senate.gov/imo/media/doc/15-05%20-%201-29-15.pdf (opening statement of Dr. Henry A. Kissinger, Chairman of Kissenger Associates and former Secretary of State) [hereinafter *Senate Armed Services Testimony*].

point out that we are living through a time of monumental change across the world."[6]

We are not operating in an absolute vacuum, however. As President Obama noted in his 2010 National Security Strategy report: "Time and again in our Nation's history, Americans have risen to meet—and to shape—moments of transition."[7] Obama's remarks echo the sentiments of President Bush in his 2006 National Strategy Report when he noted that as a nation "[w]e have seen great accomplishments, confronted new challenges, and refined our approach as conditions changed" in a way that both presidents would agree is inspired by the ideals of our history—freedom, democracy, and human dignity. Dr. Kissinger expressed a similar position noting that, despite the myriad challenges to our national security, "[b]y any standard of national capacity, [the United States is] in a position to achieve our objectives and to shape international relations."[8]

America's last two presidents, while having vastly different perspectives on foreign and national policy, have both recognized within their national security strategies that we are in unprecedented times of globalization. And we have seen the good that can come from such globalization—advances in medicine, technologies, and the peaceful spreading and growing of democracies throughout the world. We also have witnessed the dark side of globalization—the intrusiveness of technology on privacy and other civil liberties, the rise of cyber threats, external threats from natural disasters and disease, and the threats that come from those suffering under inequality, economic instability, and religious extremism. Secretary Albright recently commented on these two sides of globalization: "[The United States is] reckoning with new forces that are pushing humanity down the path of progress, while also unleashing new contradictions on the world scene."[9]

Thus our "interconnectedness" has made our national security all the more dependent on our role in the world and the choices we make. On the one hand, do we display confidence and perhaps a sense of isolationism as suggested by President Bush's national security strategy? Or, do we, as President Obama has said, face the world as it is and work within it? Do we use what has made us great in the past—sturdy alliances, an unmatched military, the world's largest economy, a strong and evolving democracy, and a dynamic citizenry to protect and strengthen our national security? As Secretary Albright

[6] *Id.* at 9 (statement of Secretary Madeleine K. Albright, Chair of the National Democratic Institute and former Secretary of State).

[7] NATIONAL SECURITY STRATEGY, WHITE HOUSE 12 (2010), *available at* https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[8] *Senate Armed Services Testimony*, *supra* note 5, at 30 (opening statement of Dr. Henry A. Kissinger).

[9] *Id.* at 9 (statement of Secretary Madeleine K. Albright).

stated in her testimony before the Senate Armed Services Committee, "We are the only nation with not just the capacity and will to lead, but also the ideals to do so in a direction that most of the world would prefer to go—towards liberty and justice, peace, and economic opportunity for all."[10]

In the legal profession, success (and failure) is measured, at least in part, by our ability to analogize our client's particular set of facts to those of previous cases—precedent—to show how our case should fit within the established framework. We prefer certainty—a framework with few surprises that can predict the legal future by relying on the legal past. And in those instances where an opinion or decision takes us in new directions, we often claim that it is not in fact avulsive but rather a logical outcome from all that has come before.

But the question becomes, particularly in the national security context, is this gradual, carefully calibrated, and measured approach to building a legal framework that will guide, protect, and foster our national security always the right approach? How do we ensure embodiment of and adherence to the basic principles of humanity and democracy that our Founding Fathers valued in the Constitution in a 21st century world that is so vastly different than anything we could have perhaps imagined even fifty years ago?

Simply stated—and again to borrow from the law of property—should our national security legal framework be one based on avulsion or accretion? Is there some happy medium, and if there is, how do we get there?[11] These are some of the larger themes and questions addressed during the Symposium and throughout the pieces in this edition.

[10] *Id.* at 10–11.

[11] During both the Senate and House Armed Services Committee hearings on the United States national security strategy, witnesses testified that a successful national security strategy must be one that does not simply react to the crisis of the day or month, but rather be focused on long-term priorities and commitments. *See, e.g.*, *Global Challenges and the U.S. National Security Strategy Before the Senate Armed Services Committee*, 115th Cong. 3, at 37 (2015) (testimony of William J. Fallon) ("We should resist reactive responses and attempts to find near term fixes for pop issues which arise continuously and compete for attention with what we should determine are higher priority interests"), http://www.armed-services.senate.gov/imo/media/doc/15-03%20-%201-27-15.pdf. Examining the strength of our national security legal framework is in keeping with this advice. Similarly, in the 2015 National Security Strategy, President Obama noted that in order to succeed in securing Americans, "we must draw upon the power of our example—that means viewing our commitment to our values and the rule of law as a strength, and not an inconvience." Barack Obama, *Preface* to 2015 NATIONAL SECURITY STRATEGY, WHITEHOUSE (2015), *available at* https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf [hereinafter 2015 NATIONAL SECURITY STRATEGY].

II. Intelligence Gathering, Big Data, and the Threat to Privacy

Intelligence gathering operations—both U.S. and international—have never been greater. Lieutenant General William C. Mayville, Jr., the Director of Operations for the Joint Chiefs of Staff, testified before the House Armed Services Committee that the demand for intelligence, both on and off the battlefield, is "insatiable."[12] In the digital age, average citizens routinely throw around the term "big data" as they upload pictures to Instagram, change their status on Facebook, and follow their favorite celebrities on Twitter. We are voluntarily and mandatorily under surveillance in virtually every aspect of our lives.

In their piece, *Security, Privacy, and Technology Development: The Impact on National Security*, Abraham R. Wagner and Paul Finkelman introduce us to the "revolution" and "evolution" of modern communications and information technology: the growth of big data and its impact on our ideas of privacy and security. The authors note, "For most of history people have had very little to keep private. Literacy was limited, communications were costly and even more limited, and there was no Big Data."[13] Wagner and Finkelman explore not only the development of big data but how we, as users and used, have changed our views of privacy and security in the age of modern communications. Wagner and Finkelman provide the constitutional and legal underpinnings of our idea of "privacy" and how technology—from the dawn of the photograph to the age of Snapchat—has altered our view of "privacy" and the legal doctrines that protect it.

Wagner and Finkelman posit, "in many respects the legal regime [with respect to privacy] is several generations behind current technology and how it is being utilized."[14] In their words, "the United States has been incredibly tardy in passing legislation responding to new Internet technology."[15] They point to several key areas in which the United States could be more robust in its national security and privacy efforts: understanding and appreciating threats from cyber warfare; recognition of the role of cyberspace in a dynamic world; building a better technological base through significant higher education efforts in the field of technology; funding more security initiatives for the cyber world—particularly as the U.S. federal government is the largest user of the Internet; and exploring more robust and engaged part-

[12] Lieutenant General William C. Mayville, Jr., Oral Testimony, House Armed Services Committee on Worldwide Threats (Feb. 3, 2015), *available at* http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=9894B134-0765-484C-AB5F-882D4410ACD2.

[13] Abraham R. Wagner & Paul Finkelman, *Security, Privacy, and Technology Development: The Impact on National Security*, 2 Tex. A&M L. Rev. 597, 611 (2015).

[14] *Id.* at 612.

[15] *Id.* at 614.

nerships with private industry, including a "national policy and legal regime that recognizes the role that industry [technology such as servers and clouds] ha[s] in maintaining Big Data and protecting both the privacy of users and security of their data."[16]

The issues associated with big data and our legal framework discussed by Wagner and Finkelman are inherent in our national security strategy. According to documents provided to media outlets by Edward Snowden, the Fiscal Year 2013 National Security Assessment, which had never before been released publicly, the U.S. has funded a $52.6 billion intelligence gathering operation spanning sixteen agencies and comprising of over 100,000 employees.[17] Given this labyrinth of surveillance, how do we protect from the types of intrusion and government overreach that James Madison might have included in his observation: "Since the general civilization of mankind, I believe there are more instances of the abridgment of the freedom of people by gradual and silent encroachments of those in power than by violent and sudden usurpations."[18]

III. Traditional Threats from Non-traditional Sources

The threat from traditional national security challenges such as nuclear war and proliferation of weapons of mass destruction in rogue nations continue to top the priorities of our national security apparatus. According to the 2015 National Security Strategy, "No threat poses as grave a danger to our security and well-being as the potential use of nuclear weapons and materials by irresponsible states or terrorists."[19] Some have suggested that, at least with respect to nuclear conflict, "everything on this side of the nuclear divide is new."[20] But it may be that it is not so much that the *threat* is new as it is that, like our ability to access information far faster and in far greater quantities than ever before imagined, the material is more readily available.[21]

[16] *Id.* at 632.

[17] Barton Gellman & Gregg Miller, *'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives*, Wash. Post (Aug. 29, 2013), http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

[18] 11 James Madison, Speech in the Virginia Convention, Richmond, Virginia (June 6, 1788), *in* The Papers of James Madison 78, 79 (Robert A. Rutland & Charles F. Hobson eds., 1978).

[19] 2015 National Security Strategy, *supra* note 11, at 11.

[20] Peter Paret, *Introduction* to Makers of Modern Strategy: From Machiavelli to the Nuclear Age 7 (Peter Paret et al. eds., 1986) [hereinafter Makers of Modern Strategy].

[21] 2006 National Security Strategy of the United States of America, Whitehouse 20 (2006), *available at* http://www.comw.org/qdr/fulltext/nss2006.pdf (noting that "nuclear weapons represent a 60-year old technology and the knowledge [for creating such weapons] is widespread") [hereinafter 2006 National Security Strategy].

"Cold War stockpiles remain. More nations have acquired nuclear weapons . . . . Black markets trade in nuclear secrets and materials."[22] It is far "easier" now for terrorist or other rogue entities to obtain nuclear material—thus making a threat of terrorist attack using a WMD one of the greatest.[23] This access to materials has resulted in terrorists being more "determined to buy, build, or steal a nuclear weapon."[24]

These threats are not necessarily "new" in the typical sense of the word, but the way in which they threaten our national security can be perceived as such. Dr. Kissinger addressed this in his opening remarks to the Senate Armed Services Committee's hearing on Global Challenges and the U.S. National Security Strategy, "[T]he nature of strategy has shifted—from an emphasis on objective strength, to include a major component defined by psychological contests and asymmetric war."[25]

As one would expect, the intelligence community grew considerably after the terrorist attacks of September 11, 2001. As Director of National Intelligence James Clapper noted in his response to the *Washington Post*'s release of the 2013 National Security Assessment:

> The United States has made a considerable investment in the Intelligence Community since the terror attacks of 9/11, a time which includes wars in Iraq and Afghanistan, the Arab Spring, the proliferation of weapons of mass destruction technology, and asymmetric threats in such areas as cyber-warfare.[26]

More access to the underlying material or "know-how" is an ongoing threat to national security and the delivery methods that raise questions about the adaptability of our legal framework and national security infrastructure to respond to 21st century threats. As Tung Yin explains in his piece, *Game of Drones: Defending Against Drone Terrorism*, prior to the attacks of September 11, 2001, the use of airplanes as terror-delivery systems had appeared in at least two blockbuster novels.[27] Novels, movies, and television programs all present scenarios in which "dirty bombs" explode in crowded sports arenas or at other public events.

Imagine this scenario:

> *It is a cold, rainy night in January. At approximately 3:00 a.m., the entire White House complex is locked down, Secret Service agents are*

[22] 2010 National Security Strategy, Whitehouse 23 (2010).

[23] 2006 National Security Strategy, *supra* note 21, at 18; 2010 National Security Strategy, *supra* note 22, at 23.

[24] 2010 National Security Strategy, *supra* note 22, at 23.

[25] *Senate Armed Services Testimony*, *supra* note 5, at 30 (opening statement of Dr. Henry A. Kissinger).

[26] Gellman & Miller, *supra* note 17.

[27] Tung Yin, *Game of Drones: Defending Against Drone Terrorism*, 2 Tex. A&M L. Rev. 635, 637–38 (2015).

> *scrambled, and emergency personnel and other law enforcement descend upon the Southeast entrance to the White House. The threat? A two-foot-long "quadcopter" drone that crashed onto the White House lawn.*

Another plot in a novel? No. On January 26, 2015, a civilian accidentally crashed a private drone on the White House grounds causing its security apparatus to go on full alert. While a harmless accident, the drone intrusion exposed significant weaknesses in White House security and our ability to respond to threats from such a non-traditional source.

It is exactly such an occurrence that Yin considers in his piece. Yin's analysis is incredibly timely in light of this most recent breach of White House security, as it provides an important overview of the threat posed by domestic drone terrorism and "the technological and legal issues involved in setting up defensive responses" to it.[28] As Yin explains, when the U.S. introduced the era of "weaponized drone warfare" it also "opened Pandora's Box" to the possibility that the "United States may soon find itself on the wrong end of a weaponized drone."[29]

Yin's piece is prescient in its review of existing laws and regulations regarding private (civilian) drones and proposals "to develop the legal and technological architecture to defend against drone terrorism." As Senator Charles Schumer announced the day after the White House incident, "There is no stronger sign that clear FAA guidelines for drones are needed."[30]

The flipside of the domestic drone threat is, of course, that unmanned aerial vehicles, or "remotely piloted vehicles" as they are called by the United States Air Force, have become an important part of the U.S. weapons arsenal. In David E. Graham's piece, *The U.S. Employment of Unmanned Aerial Vehicles (UAVs): An Abandonment of Applicable International Norms*, Graham explores the use of drones as a weapons system by the United States.[31] Both Yin and Graham note that the dialogue surrounding the use of drone technology often blurs between a discussion of the system itself and the policies supporting its use.[32] Graham posits in his piece that if there is any perceived uncertainty about the legitimacy of the system or whether current legal norms (both international and domestic) are sufficient to

[28] *Id.* at 638.

[29] *Id.* at 636.

[30] *Man Claims Responsibility for Drone Crash at White House, Says was an Accident*, FOX NEWS (Jan. 26, 2015), http://www.foxnews.com/politics/2015/01/26/obama-spokesman-says-device-found-on-white-house-grounds-poses-no-threat.print.html.

[31] David E. Graham, *The U.S. Employment of Unmanned Aerial Vehicles (UAVs) and Abandonment of Applicable International Norms*, 2 TEX. A&M L. REV. 675, 676–78 (2015).

[32] Yin, *supra* note 27, at 641; Graham, *supra* note 31, at 679.

govern its use against those who threaten U.S. national security interests, it is an uncertainty of our own making.[33]

Graham provides significant background on the current state of UAVs as a weapons platform and notes that the UAV "is simply one of any number of weapon platforms" available to the United States.[34] Graham asserts that criticism of U.S. drone use has never been about the legitimacy of the platform, but the legal basis on which its use is authorized. Graham explores the development of the U.S. legal justifications for drone use and its targeting of certain individuals and provides a critique of the underlying analysis. Graham suggests that existing international legal principles and frameworks regulating a State's use of force provide sufficient legal basis for our actions, but that our own hesitancy and legal analyses have led to uncertainty about their legitimacy. According to Graham, the existing legal framework and principles can work so long as the United States does not "ignore[ ], misinterpret[ ], or misappl[y]" them.[35]

IV. Asymmetric Warfare[36] & Intelligence Gathering in the 21st Century

According to the 2013 National Security Assessment, approximately 13% of the Intelligence Community's budget went to "counter weapons proliferation."[37] As detailed in the National Security Assessment, the intelligence community—particularly the NSA and CIA—have taken a more aggressive approach to asymmetric threats like cyber security by not simply "spying" on foreign systems and entities trying to infiltrate U.S. interests, but proactively hacking foreign com-

[33] Graham, *supra* note 31, at 679.

[34] *Id.* at 678; *see also* Yin, *supra* note 27, at 638–40; Chris Jenks, *Law From Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict*, 85 N.D. L. Rev. 649, 652–53 (2009) (explaining that the Department of Defense defines UAV as "a powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and carries a lethal or nonlethal payload" (citation omitted)).

[35] Graham, *supra* note 31, at 679.

[36] Asymmetric warfare or asymmetric armed conflict can be defined as involving a "State on the one hand and a non-State entity on the other." David E. Graham, *The Law of Armed Conflict in Asymmetric Urban Armed Conflict*, 87 Int'l Law Stud. 301, 302 (2011); *see also* Franklin B. Miles, Asymmetric Warfare: An Historical Perspective 2–3 (1999) (setting forth DOD and CIA definitions of asymmetric warfare and noting that their commonalities include pitting one's strengths against an opponent's weaknesses and using "unexpected, unconventional, or innovative methods of attack or defense"), *available at* http://www.hsdl.org/?view&did=439201.

[37] Gellman & Miller, *supra* note 17; *see also* 1 Fiscal Year 2009: Congressional Budget Justification, U.S. Office of the Director of National Intelligence 9 fig.1 (2012), *available at* http://www.scribd.com/doc/164056434/FY-2013-Congressional-Budget-Justification.

puter networks to either obtain more data from them or sabotage them altogether.[38]

General Vincent R. Stewart, the director of the Defense Intelligence Agency observed during testimony before the House Armed Services Committee, "The theft of intellectual property is as old as the world itself. Now we are just doing it in cyber space."[39] In today's world, the United States must now recognize that "nation states are trying to damage our networks [and access our intellectual property]" every day; "the challenge is how to see the threat more discretely. . . . We don't see the threat early enough."[40] As Mark S. Chandler, Acting Director of Intelligence for the Joint Chiefs of Staff, commented, the cyber environment is so complex that early detection of cyber threats is hard but absolutely necessary.[41]

Intelligence gathering has always been as much about knowing one's allies as one's enemies. In the international arena, however, this accepted custom does not come without cost. The National Security Assessment outlines in great detail foreign states that have been identified as top targets for intelligence gathering. The list includes allies such as Israel and Pakistan. The proliferation of recent "big data" disclosures have made clear that even allies such as Germany do not escape notice by the intelligence communities. As General Mayfield observed during his testimony before the House Armed Services Committee, today's demand for intelligence is insatiable.

Thus one question considered by Symposium participants is whether the existing international legal framework is able to adapt to and curtail rapidly developing threats from surveillance and cyber espionage.

V. Emerging Biotechnology & The Law: Are We Keeping up with the Biotechnology Revolution?

It really began with the discovery of the double helix in the 1950s: a revolution in biotechnology that has brought with it the prospect of

[38] Gellman & Miller, *supra* note 17; *see also Worldwide Threats Before the H. Armed Servs Comm.*, 114th Cong. 22 (Feb. 3, 2015) (statement of Lieutenant General Vincent Mayfield, Director, Defense Intelligence Agency) (noting that the "absence of universally acceptable and enforceable norms in cyberspace" contribute to threats to cybersecurity and, as a result, "states worldwide are forming 'cyber command' organizations and developing national capabilities"), *available at* http://docs.house.gov/meetings/AS/AS00/20150203/102880/HHRG-114-AS00-Wstate-StewartUSMCV-20150203.pdf

[39] Lieutenant General Vincent R. Stewart, House Armed Services Committee on Worldwide Threats (Feb. 3, 2015), *available at* http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=9894B134-0765-484C-AB5F-882D4410ACD2.

[40] *Id.*

[41] Mark S. Chandler, House Armed Services Committee on Worldwide Threats (Feb. 3, 2015), *available at* http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=9894B134-0765-484C-AB5F-882D4410ACD2.

great advancements in human health and the potential for great harm. "Biotechnology is one of the world's fastest growing commercial sectors."[42] As it relates to national security, biotechnology that has a "dual use"[43] provides both the potential for use as part of a country's strategic arsenal[44] and great harm to the citizenry. The United States government's oversight of such technology "is aimed at preserving the benefits of life sciences research while minimizing the risk of misuse of the knowledge, information, products, or technologies provided by such research."[45] The literal explosion in the fields of biotechnology, and our experiences with the anthrax attacks in 2001 and the Ebola scare of 2014, raise significant questions about the capability of our existing national security and legal frameworks to protect and adapt to the ever-increasing field of biotechnology.

In her piece, *Emerging Biotechnologies and the 1972 Biological Weapons Convention: Can It Keep Up with the Biotechnology Revolution?*, Dr. Victoria Sutton explores the growth of biotechnology and the legal structures designed to regulate it—specifically the 1972 Biological Weapons Convention. Dr. Sutton sets forth the history of the Convention and notes that even in its earliest days, States were concerned about "dual use" biotechnologies and the possibility of harm arising from the good in the biotechnology revolution[46] but that, for the most part, States believed the Convention was sufficient to prevent the misuse of biotechnology for biowarfare.[47]

[42] James J. Carafano & Andrew Gudgel, *National Security and Biotechnology: Small Science with Big Potential*, rep. no. 2055, HERITAGE FOUNDATION (July 23, 2007), http://www.heritage.org/research/reports/2007/07/national-security-and-biotechnology-small-science-with-a-big-potential.

[43] According to the National Institutes of Health, "dual use research of concern" is defined as—

> life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security.

Biosecurity: Dual Use Research Concerns, NAT'L INSTS. OF HEALTH, OFFICE OF SCI. POLICY, http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/dual-use-research-concern (last visited June 15, 2015) [hereinafter *Biosecurity: Dual Use Research Concerns*].

[44] *See* Carafano & Gudgel, *supra* note 42, at 4 ("Before 2001, the Department of Defense (DOD) was the primary arm of the federal government [—] funding biological defense and research related to national security.").

[45] *See Biosecurity: Dual Use Research Concerns*, *supra* note 43.

[46] *See* Victoria Sutton, *Emerging Biotechnologies and the 1972 Biological Weapons Convention: Can it Keep Up with the Biotechnology Revolution?*, 2 TEX. A&M L. REV. 695, 699 (2015) (discussing State party observations in 1980 about the role of the Convention in monitoring and regulating dual use developments including "genetic engineering).

[47] *Id.* at 700 (noting that the 1980 review of the Convention concluded that it was sufficient to cover emerging technologies and not susceptible to covert violation or bypass and explaining that, in fact, countries like the former Soviet Union were actively engaged in practices that violated the Convention).

Dr. Sutton traces the subsequent meetings of the States with respect to the Convention explaining that at each meeting, the States agreed that the Convention "applies to all scientific and technological developments in the life sciences and in other fields of science relevant to [it]."[48] As Dr. Sutton explains, the emerging complexity of the biotechnology sphere has likewise increased the complexity and coverage of the Convention. For example, Dr. Sutton questions whether Article I of the Convention covers "invasive species" (as it does cover genetically modified mammals and insects) and the implications of using invasive species as a form of biological weapon. She also suggests that despite the ever-expanding definition of technologies covered by the Convention, bionanotechnologies and nanobiotechnologies (fields involving materials so small that they are invisible to the naked eye) may literally escape notice under the Convention. For example, Dr. Sutton notes that if the material lacks sufficient biological components, it would not fit the Convention's definition and thus remain a very real threat.[49] Dr. Sutton also suggests that advancements in certain physiological and psychological substances, currently part of the military's biotechnology, may fall outside the scope of the Convention.[50]

Dr. Sutton's piece also explains that with this rapidly increasing field of biotechnology comes the need for more "verification protocols" and "confidence building measures," calls for which are increasing from those States without robust biotechnology industries.[51] She suggests that the Convention's definition of covered materials is now so broad that the plain meaning articulated in 1972 may be lost and, as such, significant threats from emerging technologies may go undetected. As a result, Dr. Sutton suggests that the existing legal framework should be re-evaluated.[52]

VI. Mass Surveillance & Its Impact on Privacy and Community

Perhaps it is the open—if somewhat forced—acknowledgement that we are, in fact, gathering information on everyone all the time that has some questioning what national security really means. Have we in a post-9/11 world surrendered all of the ideals and core values, including our belief in the sanctity of privacy to the interests of national security? Does the right to privacy remain the bedrock of this nation's government and society? In this age of Snapchat, Twitter, Facebook, and Instagram through which we can literally update everyone in the world about our actions, likes, fears, and dreams twenty-

[48] *Id.* at 708 (quoting the Seventh Review Conference Report of 2011).
[49] *Id.* at 716–18.
[50] *Id.*
[51] *Id.* at 713.
[52] *Id.* at 718.

four hours a day, what does *privacy* mean? And how do we weigh *privacy* against *national security*? Wagner and Finkelman, discussed *supra*, address both of these issues and note that the physical world of letters, books, newspapers, and "virtually anything else that once existed as paper or plastic are now digital files that are stored and downloaded."[53] This digital age raises the question not only whether there is "privacy" but privacy from whom?[54]

In their piece, *National Security, Narcissism, Voyeurism, and* Kyllo: *How Intelligence Programs and Social Norms are Affecting the Fourth Amendment*, Adam Pearlman and Erick Lee address the "legal quandaries" created by advanced technology and our ever-growing dependence on web-based social networking.[55] From tort law to intellectual property, traditional-legal frameworks have expanded to encompass the impact of social media. Pearlman and Lee note that criminal law and national security have been extraordinarily impacted by the growth of social media. On the one hand, social media has provided the government an expansive new tool and resource for the detection of criminal activity, but on the other hand, it seems that the collection of mass data and other information has resulted in a world in which the citizenry have no privacy at all. Pearlman and Lee attempt to strike a balance between government use of social media and the citizenry's desire for "privacy," and suggest that privacy is—and perhaps always has been—a "legal fiction" but is one that should be protected to the extent possible, even as people seem more willing to give up their privacy on social media.[56]

In their piece, Pearlman and Lee trace the history of the Fourth Amendment and the development of both the legal framework for and society's notion of the "right to privacy" in the context of advancing technologies, specifically noting that some of the earliest Supreme Court decisions in this area recognized "that Congress and the laws must be malleable enough to adapt to legal realities in a changing world"[57] but explaining that the history of Fourth Amendment jurisprudence and the "right to privacy" has been neither straight nor easy. Pearlman and Lee then show the parallel growth of mass surveillance and national security and the attempts of our legal frameworks to keep up, noting that as technology evolves and external threats materialize, society seems more willing to give up some "privacy" for the betterment of "national security." Pearlman and Lee then conclude that society's willingness to sacrifice "privacy" both in our growing

[53] Abraham R. Wagner & Paul Finkelman, *Security, Privacy, and Technology Development: The Impact on National Security*, 2 TEX. A&M L. REV. 597, 612 (2015).

[54] *Id.* at 612–13, 619.

[55] Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and* Kyllo*: How Intelligence Programs and Social Norms are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 720 (2015).

[56] *Id.* at 723.

[57] *Id.* at 726 (internal citation omitted).

reliance on social media and its pervasiveness in every aspect of life and in our willingness to give law enforcement more access has fundamentally changed what a "reasonable" expectation of privacy is in the 21st century.

Sahar Aziz considers all of the questions raised during this Symposium in her concluding remarks. She specifically targets the questions in the context of the impact of overbroad surveillance and other intelligence gathering activity domestically and internationally, and she particularly highlights the travails faced by Muslim communities since the 9/11 terrorist attacks.[58] Aziz explores these interrelated themes of national security, community, and privacy and suggests that much of what we are doing in the name of national security is actually detrimental not only to our national security interests but those core values on which our government is supposed to be based.

She remarks on the rise of the national security industrial complex and explains that domestic and international surveillance activities and anti-terrorism programs have resulted in stereotypes, particularly of Muslim communities, created negative attention for them, and ultimately, not been effective in identifying or preventing terrorist attacks.[59] She further explains how overbroad surveillance activity, and racial profiling in the counterterrorism contexts create a culture of fear that prevents "our government's ability to provide equal protection under the law to all persons" and can lead, as did the government's deeply flawed policies of domestic Japanese internment during World War II, to the compromise of "our nation's rule of law."[60] Professor Aziz reminds us most eloquently that we must be vigilant in our consideration of national security interests and mindful of the very real possibility that internal threats to our civil liberties may be equal to or greater than external threats to our security interests.

VII. Conclusion

No matter what the new national security "threat" or technology may be, it is wise to remember that every age is "unique in its combination of conditions, issues, and personalities; . . . a profound revolution in technologies, beliefs, or in social or political organization [may seem] to sever us from history . . . [b]ut history as the educated memory of what has gone before is a resource not to be abandoned

[58] *See* Sahar F. Aziz, *Security and Technology: Rethinking National Security*, 2 Tex. A&M L. Rev. 791, 793–95 (2015) [hereinafter Aziz, *Rethinking National Security*].

[59] *Id.*; *see also* Sahar Aziz, *Did Religious Profiling Allow Paris Terrorists to Proceed Undetected?*, Huffington Post: WorldPost (Jan. 9, 2015), http://www.huffingtonpost.com/sahar-aziz/did-religious-profiling-allow-paris-terrorists-to-proceed-undetected_b_6435812.html.

[60] Aziz, *Rethinking National Security*, *supra* note 58, at 794.

lightly."[61] With respect to a nation's security and its relations with other states, "the present always has a past dimension, which it is better to acknowledge than ignore or deny."[62] Thus, the articles contained in this Symposium Edition significantly contribute to the discussion of national security by exploring the advent of new technologies and threats in the context of our established legal frameworks and addressing the question: *How do we think about national security?* This special Symposium Edition and the issues, challenges, and solutions discussed therein contribute significantly to the review currently being undertaken of our national security strategy.

The *Texas A&M Law Review* is extraordinarily grateful to the presenters and authors who have contributed to this special edition and to the greater dialogue about national security and its legal frameworks.

[61] Makers of Modern Strategy, *supra* note 20, at 8.

[62] *Id.*