American University Law Review

Volume 62 | Issue 5 Article 2

2013

Leap-Ahead Privacy as a Government Responsibility in the Digital Age

Ivan K. Fong

David G. Delaney

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aulr

 Part of the Law Commons

Recommended Citation

Fong, Ivan K.; Delaney, David G. "Leap-Ahead Privacy as a Government Responsibility in the Digital Age." American University Law Review 62, no.5 (2013): 1131-1144

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

Leap-Ahead Privacy as a Government Responsibility in the Digital Age

Keywords
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, Keynote Transcript, Fong, Ivan K., Delaney, David G., Government liability -- United States, Right of privacy -- United States, Disclosure of information -- Law & legislation -- United States, Computer crimes -- United States

This article is available in American University Law Review: http://digitalcommons.wcl.american.edu/aulr/vol62/iss5/2

KEYNOTE TRANSCRIPT

"AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD"

LEAP-AHEAD PRIVACY AS A GOVERNMENT RESPONSIBILITY IN THE DIGITAL AGE

IVAN K. FONG* & DAVID G. DELANEY**

Thank you for your invitation to speak at today's symposium, whose theme, "America the Virtual: Security, Privacy, and Interoperability in an Interconnected World," is without a doubt both timely and important. The issues you are discussing and debating here are central, not only to industry, government, and the academic community in general, but also to the Department of Homeland Security ("DHS" or "Department") in particular. One of the Department's five core missions, after all, is to safeguard and secure cyberspace. And it is no exaggeration to say that "[o]ur daily life, economic vitality, and national security depend on a safe, secure, and resilient cyberspace."[1]

It is also no exaggeration to state that our nation faces significant and

---

* Although Mr. Fong delivered these remarks after his departure from his position as General Counsel of the U.S. Department of Homeland Security in October 2012, they were prepared by Mr. Fong in his official capacity during his tenure with DHS and thus represent views consistent with those of the Administration.

** Deputy Associate General Counsel, U.S. Department of Homeland Security. The authors wish to thank Bruce McConnell, Matthew Angelo, and Lynn Parker for their substantial assistance with these remarks.

1. *Understanding the Homeland Threat Landscape: Hearing Before the H. Comm. on Homeland Sec.*, 112th Cong. 16 (2012) (testimony of Janet Napolitano, Sec'y, U.S. Dep't of Homeland Sec.), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Napolitano_0.pdf.

increasing cyberthreats from a range of individual, organized, and state actors. Recent headlines remind us, for example, that malicious actors can easily render tens of thousands of computers inoperable, as was done to Saudi Aramco in August of this year; that distributed denial of service attacks can significantly degrade web services, as was done to several major U.S. banks last month; and that hackers can penetrate the networks of companies operating natural-gas pipelines.

The statistics on cybercrime, data breaches, and loss of personal information are sobering. This year the global cost of cybercrime has been estimated at $110 billion.[2] Between ninety-five and ninety-eight percent of records lost through data breaches contain personal information—that is, data such as names, addresses, e-mails, or social security numbers.[3] In fiscal year 2011, the Secret Service prevented $1.6 billion in potential losses through its cybercrime investigations. And just last year, the United States Computer Emergency Readiness Team, which is DHS's 24-hour cyber-watch and warning center, responded to more than 106,000 incident reports and released more than 5000 actionable cybersecurity alerts and information products to our public and private sector partners. In short, the threats to our cybersecurity are real, they are serious, and they are urgent.

The good news is that over the past four years DHS has taken significant steps to vastly improve the security of federal government information systems, enhance cybersecurity for the private sector and non-federal government entities, and promote cybersecurity nationwide, while at the same time recognizing the unique privacy concerns that exist within the cyber sphere. DHS continues to seek improvements in the ways that government is postured to address these issues, most notably through this Administration's cybersecurity legislative proposal. Although that effort failed in the Senate last August, the federal government will continue to identify the ways that the nation—through its laws, values, and institutions—can improve our cyber awareness, readiness, and capabilities.

Indeed, today's symposium occurs at a particularly fitting time, for this is the final week of National Cyber Security Awareness Month, the overarching theme of which this year is "Achieving Cybersecurity Together." The focus for this week is "Digital Literacy and Education," a perfect topic to bring to this audience. In keeping with these themes, what follows are several steps that can be taken in the coming months and years to adequately prepare for what lies ahead in this vital and dynamic field.

---

2. SYMANTEC, 2012 NORTON CYBERCRIME REPORT 6 (2012), *available at* http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

3. VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 42 (2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

* * *

It is an axiom of modern life to say that today's technological landscape is changing rapidly. These changes create significant challenges for attorneys, educators, and clients. For example, legal practitioners and clients must understand a range of evolving issues just to conduct day-to-day business—e-filing, e-discovery, and preserving privilege in the digital age are issues that are new in the last twenty years. Although the need for every law student to demonstrate expertise in both law *and* technology with respect to cyber issues may not yet be essential, it is approaching that point for attorneys who want to practice in government cybersecurity fields. At DHS, the goal is for attorneys to demonstrate not only expert legal skills, but also technological literacy and a desire to develop expertise in the operational fields they serve, to enable them to evaluate and make more sophisticated legal and policy recommendations. Government, private sector, and academic communities should understand that we share a range of interests in promoting the sound practice of law in support of national cybersecurity programs. And given the evolving nature of our highly networked, digital world, we should take time to jointly and collaboratively anticipate what the future holds so we can plan for our needs accordingly.

Over a century ago, Samuel Warren and Louis Brandeis took such an approach in their seminal article, "The Right to Privacy," arguing that advances in technology and changes in business practices necessitated a common law right to privacy. Citing the indecency and impropriety of the press and the trade in gossip they said:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[4]

It is no less true today than in 1890 that "modern enterprise and invention"[5] can create a range of personal harms that should have remedies under the law if it is to provide a path to justice and a basis for a stable, prosperous, and peaceful society. Unlike the rate of change of technology,

---

4. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

5. *Id.* at 196.

which can be exponential, changes in the law tend to be reactive, incremental, and almost always lagging.[6] What we—government and legal communities—should learn from Warren and Brandeis is their critical assessment of the state of the law and society, their creativity in proposing a solution to serve the law and society, and their courage to promote new ideas. Although we are still in the relatively early days of the virtual world, our society is already profoundly dependent on the cyber realm, so much so that we must thoughtfully examine government roles in securing and developing that realm as a function of a sovereign's duties.

This symposium presents a good opportunity to highlight two main drivers for a strong government role in cybersecurity. And borrowing a term from the research and development community, we propose that government must seek "leap ahead" approaches to privacy in these endeavors to preserve the essence of individual liberty.

* * *

Our first observation is that government necessarily has a role to play in cybersecurity, if only because governments must now be prepared to perform nearly all of their functions in cyberspace. For the Internal Revenue Service, for example, this means providing tax information and services online. For the Defense Department, this means not only maintaining their cyber networks as a function of force readiness, but also planning for the possibility that cyber networks and their supporting infrastructure will be used as part of military action. For DHS, this means understanding and addressing the cyber dimensions of the Department's five missions: preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, ensuring resilience to disasters, and, of course, safeguarding and securing cyberspace.

To achieve these missions, DHS must know and understand how terrorists, smugglers, traffickers, intellectual property thieves, and other cybercriminals use cyberspace to cause harm or engage in wrongdoing. And the Department must harness the capabilities and opportunities of cyberspace to communicate with and serve those affected by disasters. DHS does not, of course, and cannot do these things alone. It can achieve its missions only in collaboration with the homeland security *enterprise*—that is, together with federal, state, local, tribal, and territorial governments; with the academic community; with international entities; and with the

6. *See generally* Ivan K. Fong, *Law and New Technology: The Virtues of Muddling Through*, 19 Yale L. & Pol'y Rev. 443, 454–61 (2001) (book review).

private sector. These relationships are particularly vital to the Department's efforts to secure critical infrastructure and information systems. Indeed, DHS is uniquely positioned to work across the homeland security enterprise to analyze and mitigate cyberthreats and vulnerabilities; distribute threat warnings; provide solutions to key research and development needs; and coordinate the vulnerability, mitigation, and consequence-management response to cyber incidents. As a result of these efforts, DHS has become the federal government's focal point for ensuring that our computers, networks, and information systems are and remain safe for commerce, for communication, and for our national security.

In carrying out these core responsibilities, it is worth noting that DHS puts a special emphasis on protecting privacy, civil rights, and civil liberties. The Department, for example, conducts privacy impact assessments of cybersecurity programs, trains employees on privacy and civil liberties, and consults privacy experts as cyber programs are developed. Among these experts is the DHS chief privacy officer, who has independent audit authority for DHS programs and works closely with DHS officials to develop sound programs. Congress should rightly be credited for this leap-ahead approach to privacy, because the position was the first of its kind established by statute in the executive branch.[7]

DHS also aspires to a leap-ahead approach to privacy through professional development programs. DHS administers the National Initiative for Cybersecurity Education, through which the federal government strives to attract, train, and retain a skilled cyber workforce. This training and development effort is increasingly important, particularly given that the size of the Department's cybersecurity workforce increased seven-fold during the last three years. And just two weeks ago, the Department began to implement a slate of eleven recommendations from its Homeland Security Advisory Council that are aimed at further improving the Department's cyber skills and relationships with academic and professional communities. This comprehensive approach to workforce development can deliver a leap-ahead approach to privacy in cybersecurity by including a best-in-class program to instill privacy principles in all of our cyber professionals. It is as true for privacy as for security that it is better to build it in than to bolt it on.

DHS also uses technology to take a leap-ahead approach to privacy. The Analytic Framework for Intelligence, or AFI, is a new and very important

---

7. *State of Federal Privacy and Data Security Law: Lagging Behind the Times?: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs, Subcomm. on Oversight of Gov't Mgmt.*, 112th Cong. 4 (2012) (testimony of Mary Ellen Callahan, Chief Privacy Officer, U.S. Dep't. of Homeland Sec.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76066/pdf/CHRG-112shrg76066.pdf.

border security system that conducts federated query searches across the Department's multiple information systems to identify people and cargo at border crossings or ports that pose security risks to the nation, while eliminating the need to focus on those that pose no danger. Logical access controls limit an analyst's access to data linked to his or her authorized job. And records are retrieved directly from a source system, precluding the need for multiple copies of databases. These are not only good privacy practices, but good security practices, because they help us produce more *accurate* intelligence products quickly. As with the Department's approach to employee development, AFI shows how to achieve greater privacy by design.

* * *

Our second observation is that government entities have a responsibility to be alert to and address a range of macroscopic forces shaping the nation and the cyber environment. Trends in the economy, technological developments, and security capabilities all factor into the issue of whether the government should intervene, and if so, how to do so in an effective and efficient way. The current and evolving cyberthreat landscape suggests that reliance on the market alone to meet cybersecurity and privacy needs has not and will not be sufficient to achieve the goal of a secure and privacy-protective cyber environment.[8] Any argument that the collective responsibility of the market obviates the need for government guidance is belied by recent events. One reason is that cybersecurity is not yet scalable—that is, in many industries, for companies that provide critical services, the cost of implementing government- and industry-recommended best practices, such as the upgrading of cybersecurity systems, still outweighs any perceived risk-reduction benefits.

In addition, cyberthreats impose externalities. That is, they impose risks and harms *beyond* the individual entities that are directly affected. Malware on one company's network, for example, can cascade to the entire sector or the economy at large. Given the significant public and private interests at stake, the public and private sectors must therefore work

8. *See generally*, CENTER FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY: A REPORT OF THE CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY 49–59 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

together to develop industry-led, minimum baseline cybersecurity standards. As John Brennan, the President's homeland security and counterterrorism advisor, has noted:

> For decades, industry and government have worked together to protect the physical security of critical assets that reside in private hands, from airports and seaports to national broadcast systems and nuclear power plants. There is no reason we cannot also cooperate to protect the cyber systems of critical infrastructure on which our economic well-being, national security, and daily lives depend.[9]

The law itself—including statutes, regulations, and court decisions—serves as another macroscopic force in this area. Under current law, Congress gave DHS significant cyber authorities, and DHS inherited a patchwork of others. Although the law often changes subtly over time through regulatory programs or application of the common law, it can also change more significantly, when necessary, to address critical needs through legislation. Over the past several years, successive administrations have reported to the public and Congress that the current legal framework for the nation to advance necessary cybersecurity programs is significantly strained and increasingly outdated. Statutes applicable in this field include the Communications Act,[10] which dates to the era of Warren and Brandeis; the National Security Act of 1947;[11] the Privacy Act;[12] and more recent statues like the Federal Information Security Management Act,[13] the Homeland Security Act,[14] and the Cyber Security Enhancement Act,[15] all of 2002. Each of these emerged from discrete sets of interests in regulatory, military, information security, law enforcement, or counterterrorism siloes that do not adequately address the cross-cutting nature of the issues or the nation's current, urgent cybersecurity needs.

In short, we have reached a point where current threats and the need for strategic approaches to the nation's cyber interests render our existing amalgam of laws inadequate. The Administration's recent cybersecurity legislative proposal offered a detailed roadmap for Congress to begin to

---

9. Letter from John Brennan, Asst. to the President for Homeland Sec. and Counterterrorism, to Chairman Jay Rockefeller, Sen. Comm. on Commerce, Sci. and Transp. (Sept. 12, 2012), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=f4da0411-6fb3-4f2b-b3d5-0fd6767ec8db.

10. Pub. L. No. 73-416, 48 Stat. 1064 (1934), *amended by* the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56.

11. Pub. L. No. 80-253, 61 Stat. 495 (1947).

12. Pub. L. No. 93–579, 88 Stat. 1896 (1974).

13. Pub. L. No. 107–347, Title III, 116 Stat. 2899, 2946 (2002).

14. Pub. L. No. 107-296, 116 Stat. 2135 (2002).

15. Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156 (2002).

take a more comprehensive approach to these issues. It would have provided for the establishment of baseline cybersecurity practices for the nation's critical core infrastructure. Unfortunately, Congress's inability to act decisively and with foresight in this area may prove to be the most significant government obstacle to improving the state of the nation's cybersecurity.

* * *

As the Administration looks for additional opportunities to advance a legislative solution in this important area, it obviously also keeps a watchful eye on trends emerging in case law that affect its ability to achieve its missions. Cases related to border security counterterrorism programs, for example, and the use of electronic devices for administrative and law enforcement purposes, guide government officials both in using cyber capabilities to perform government functions and preserving our interests in privacy, civil rights, and civil liberties.

The Supreme Court's decision earlier this year in *United States v. Jones*[16] stands as a prime example. In *Jones*, the Court held that the government's warrantless use of a global positioning device to track the public movements of a criminal suspect, over a four-week period, was an unconstitutional search and seizure under the Fourth Amendment. Although Justice Scalia's majority opinion relied on a common law theory of trespass to find a Fourth Amendment violation, Justice Sotomayor's concurring opinion serves as a harbinger of future privacy considerations in this area. She noted that a physical intrusion is now unnecessary for many forms of surveillance and that even cases involving short-term monitoring will require particular attention with respect to application of the reasonable-expectation-of-privacy standard.[17] As a result of new technology, she noted, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[18]

Do people reasonably expect that the government might, without a warrant, track their movements in a manner that would allow their political and religious beliefs and their personal behaviors to be ascertained? Does the answer change if such collection is done in the virtual world of cyber infrastructure rather than the physical world of Jeeps and public roads? How long should law enforcement entities be permitted to retain and search such data for law enforcement purposes? Can they share such data with other government entities, or use such data when obtained by other

16. 132 S. Ct. 954 (2012).
17. *Id.* at 955–56.
18. *Id.* at 957.

government entities for non-law enforcement purposes? There are no bright-line answers to these questions. But these are the kinds of questions the Supreme Court is asking and that those in law enforcement, in government generally, and you in the academic community need to help answer.

The *Jones* case illustrates the growing tension—indeed collision is not too strong a word—between settled legal doctrines and advances in technology.[19] Just as Brandeis and Warren noted in 1890, "modern enterprise and invention" can subject an individual to far greater "mental pain and distress" than can be "inflicted by mere bodily injury."[20] In particular, the line between what is public and what is private is no longer a clear one. Rather, with modern technology, what used to be considered a binary distinction under the law—in which what is not private is, by definition, public—must now be reconsidered in light of how people today actually share information about themselves.

Courts have long held that individuals have no expectation of privacy over information voluntarily disclosed to third-parties.[21] Under this third-party doctrine, details such as your location on public streets, which you share with those who see you, and the websites you visit, which you share with your Internet service provider, are by default public. That means that you do not have a reasonable expectation of privacy over such information, and accordingly law enforcement may be permitted to obtain that information about you without a warrant. When people share information today, however, they often contemplate sharing information only with certain categories of people. They may use privacy control settings, for example, that allow information to be disseminated more broadly to family and close friends and less broadly to others, if at all. In these and other similar situations, users do not intend for all information to be "public" in the traditional sense. Instead, "controlled disclosure" is a more accurate way to think about how people share information in cyberspace today, and the law must therefore adapt to that reality.

To the extent the third-party doctrine rests on assumptions about how information is shared today that are no longer valid, the doctrine of practical obscurity likewise rests on increasingly tenuous assumptions. Over twenty years ago, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[22] the Reporter's Committee sought

19. *See, e.g.*, Fong, *supra* note 6, at 456 (noting areas where "modern-day courts and lawyers are similarly struggling to fit new technologies into existing legal conceptual rules and categories").

20. Warren & Brandeis, *supra* note 4, at 196.

21. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

22. 489 U.S. 749 (1989).

access under the Freedom of Information Act to an individual's "rap sheet" maintained by the FBI, arguing that it should be disclosed because, among other reasons, it contained information publicly available at the relevant courthouses.[23] Ruling for the government, however, the Supreme Court held that the rap sheet was properly withheld under an exception to the Freedom of Information Act; even though some information it contained might technically be considered public, there is a high privacy interest in maintaining the practical obscurity of personal information in the rap sheet.[24]

Technology has, of course, rendered this privacy-protective aspect of practical obscurity increasingly tenuous. The ability to aggregate and instantaneously search for previously obscure data erodes any assurance that information available only to a select few will not now be subjected to broad dissemination. A notable recent example is the Stop Trading on Congressional Knowledge ("STOCK") Act, signed into law in April of this year.[25] In addition to restricting Congress from engaging in certain financial transactions, the new law also requires certain financial disclosure statements submitted by senior federal officials to be posted online in a searchable database for public viewing. Before the STOCK Act, these financial disclosures were available in paper form upon request, making them public in a technical sense. It would have been difficult and impractical, however, to aggregate and disseminate broadly the sensitive information they contained. In recognition of the new reality, a district court recently delayed the implementation of the Internet posting requirement of the STOCK Act and ordered further briefing on whether this portion of the new law violates these officials' privacy rights in a way that the earlier filing requirement did not.[26]

Mindful of ways that traditional legal theories and standards are now being applied to new technologies, we are all engaged in defining privacy as a societal value and shaping the way that privacy serves as a touchstone for the development and delivery of sound public programs. We should proactively and responsibly raise questions about the application of such legal principles to situations unimagined when those principles were first articulated. And we should examine our own personal values and be prepared to articulate them as part of the national dialogue.

* * *

23. *Id.* at 760.
24. *Id.* at 780.
25. Pub. L. No. 112–105, 126 Stat. 291 (2012).
26. Senior Exec. Ass'n v. United States, 891 F.Supp.2d 745, 755–56 (D. Md. 2012).

The current generation of law students in particular is uniquely placed to help shape the future of cyber law. To prepare yourself for a future working on cybersecurity legal issues, you must first understand the law as it applies outside the cyber realm. As we survey new legal ground in cyberspace, we are constantly drawing upon analogies from other areas—privacy, search and seizure, intellectual property, and other areas. You should also learn the value of working in teams, and how to work constructively with others, for virtually everything lawyers do is through collaboration with others. And you should model your scope of vision, clarity of argument, and breadth of purpose on the likes of Warren and Brandeis. If you endeavor to serve narrow scopes and interests, you may benefit small pockets of the legal and cyber communities, but you will miss the opportunity to address the broader challenges at stake in a highly networked world.

We need the best and the brightest minds to handle the evolving nature of the threats facing the country. Few professional callings are greater than being a government lawyer, serving the public interest. Look to the Department of Homeland Security and other agencies performing cybersecurity functions to develop your professional skills. Honors programs, internships, and externships in government will give you unrivaled perspective in the cyber field as it develops. More important, being a government lawyer allows you to be part of something bigger than yourself—it is a true public service. It is an opportunity to protect and advance the rule of law, which is vitally important in homeland security and national security contexts. And you are likely to get responsibility, challenges, and opportunities earlier in your career than in other professional settings.

* * *

In closing, keep in mind two points. First, changes in technology require changes in the law and thus leadership from lawyers. In this area, government lawyers must "leap ahead" with a keen understanding of what the nation requires of its public institutions. They must then help lead their agencies and other communities to the changes that are necessary. Academic, private sector, and government communities share these responsibilities and interests, so they should strive to remain aware of the trends emerging in each. We need smart, creative lawyers who understand how to accomplish our mission while protecting civil rights and civil liberties, privacy, and the core values that define this country.

For example, when might a distributed denial of service attack constitute

an armed attack or conflict under the law of war?[27] Under what conditions would such an attack trigger a nation-state's right of self-defense?[28] And what are the limits of such responses? To what extent may online content be restricted if it offends or incites violence half-way around the world? What are the limits of "hacktivism"?[29] To what extent may the government rely on its authorities at the border to prevent, limit, or control cyberthreats originating outside the country?[30] And what is the future of Internet governance? Your critical assessment, creativity, and courage to tackle these and other fundamental issues can make you, for these topics, the Warren and Brandeis of the future.

Second, government employment in these areas is an important public service. Our nation has come together to meet great challenges before. During World War II, when our economy was mobilized for war, the American people found a way to feed themselves by growing forty percent of all the vegetables we needed in twenty million victory gardens. In the early years of the Cold War, Americans knew where the closest fallout shelter was, and we kept children indoors when polio outbreaks were the biggest threat to public health. In those times, Americans understood what was at stake; they understood that they had to contribute; and they knew that their efforts would make a difference, in ways large and small. We are likewise confronting new realities here, and we need new thinking and new energy. The world is a different place that it was fifteen years ago, before 9/11, and even ten years ago, just after 9/11.

You can contribute to those aims by joining the Department and other parts of the homeland security enterprise. Doing so is urgent; doing so is worthwhile; and doing so will undoubtedly impact our nation's economic vitality and way of life for generations. Together, we can—and we must—maintain a cyberspace that is safe and resilient and that remains a source of tremendous opportunity and growth for years and years to come. It is

---

27. *See, e.g.*, Remarks of Harold Koh, State Dep't Legal Adviser, to the the U.S. Cyber Command Inter-Agency Legal Conference, (September 18, 2012), *available at* http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/?utm_source=rss&utm_medium=rss&utm_campaign=harold-koh-on-international-law-in-cyberspace (asserting that "the *jus in bello* principle of distinction applies to computer network attacks undertaken in the context of an armed conflict" and that "States should undertake a legal review of weapons, including those that employ a cyber capability.").

28. *See, e.g.*, Remarks of Leon Panetta, Sec'y of Def., to the Business Executives for National Security, (October 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (stating that "[i]f a crippling cyber attack were launched against our nation . . . [a]nd if the Commander in Chief orders a response, the Defense Department must be ready to obey that order and to act").

29. *See* Melinda Haag, *Prosecution of Internet Hacktivist Group "Anonymous*," U.S. DEP'T OF JUST., http://www.justice.gov/usao/briefing_room/cc/mca_anonymous.html (last visited June 15, 2013) (recounting several investigations and prosecutions involving hacktivists).

30. *See, e.g.*, U.S. v. Cotterman, 709 F.3d 952, 956–57 (9th Cir. 2013).

encouraging to see such enthusiasm for these issues in the academic and professional communities; we must draw on your tremendous creativity, energy, and optimism to do something unlike what the nation has ever done before. These are complex and long-term challenges. That should not, however, be a reason for despair. It should instead motivate us to work and think and collaborate in new ways. As Albert Einstein once said, "It's not that I'm so smart. It's just that I stay with problems longer." That hints at the determination we must bring to one of today's hardest challenges.

Thank you again for this opportunity to contribute to your symposium.