

THE UNITED STATES COURTS FOR THE SECOND CIRCUIT  
2014 JUDICIAL CONFERENCE  
REPORT OF PROCEEDINGS



CYBER-SECURITY  
IN THE AGE OF  
CYBER-TERRORISM

JUNE 11-13 | SARATOGA SPRINGS, NEW YORK



# **Second Circuit Judicial Conference**

## **Report of Proceedings**

**Rapporteurs:** Harry H. Rimm, Charles Michael and Howard Master, Esqs.



United States Court of Appeals  
for the Second Circuit

CHAMBERS OF  
ROBERT A. KATZMANN  
CHIEF JUDGE

PHONE (212) 857-2180  
FAX (212) 857-2189

April 1, 2015

Dear Colleague:

From June 11-13, 2014, over 700 judges, attorneys and invited guests met to consider a critically important subject, *Cyber-Security in the Age of Cyber-Terrorism*. The gathering took place under the auspices of the 2014 Second Circuit Judicial Conference in Saratoga Springs, New York. The assembled group, which included cabinet members (past and present), two former FBI directors, a former U.S. Senator, representatives of the law enforcement community, business, and media, explored issues that are germane to the legal profession and society as a whole relating to national security, international relationships, private industry and the media.

I am pleased to provide you with a Report of the Proceedings of the 2014 Second Circuit Judicial Conference. The Conference opened with a keynote address by Homeland Security Secretary Jeh Johnson who set the stage for more discussions of our over-arching theme. This Report contains an overview of those seven panel discussions of the Conference along with the Report of our Circuit Justice, the Honorable Ruth Bader Ginsburg, biographies of the twenty new judicial colleagues we welcomed into our Second Circuit judicial family and the five colleagues to whom we bid farewell since our last circuit conference.

Under the guidance of our superb Conference Chair Judge Victor Marrero of the Southern District of New York, we had three “attorney-reporters”: Harry H. Rimm, Charles Michael and Howard Master, who attended and observed all the plenary sessions of the Conference for the purpose of generating this Report of the Proceedings of the 2014 Second Circuit Judicial Conference.

I am grateful to Judge Marrero and our three reporters, Messrs. Rimm, Michael and Master for their hard work in developing this Report of our Conference. We hope that you find this Report of the Proceedings of our 2014 Second Circuit Judicial Conference useful and stimulating.

Sincerely,

  
Robert A. Katzmann  
Chief Judge

40 Foley Square, New York, N.Y. 10007

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK  
40 CENTRE STREET  
NEW YORK, NEW YORK 10007  
(212) 805-6374

CHAMBERS OF  
VICTOR MARRERO  
UNITED STATES DISTRICT JUDGE

January 7, 2015

The Honorable Robert A. Katzmann  
Chief Judge  
United States Court of Appeals  
for the Second Circuit  
40 Centre Street  
New York, NY 10007

Dear Judge Katzmann:

I am pleased to submit the Report of the Proceedings of the Second Circuit Judicial Conference held on June 11-13, 2014 in Saratoga Springs, New York. This Report provides a summary record of each of the essential components of the Conference: your presentation on the state of the Circuit; the keynote address by the Secretary of the United States Department of Homeland Security, Jeh Johnson; the seven panel discussions which addressed the Conference topic; the report of our Circuit Justice, the Honorable Ruth Bader Ginsburg; and the judges' dialogue with Justice Ginsburg, which this year was based on a performance of arias from the opera *Scalia/Ginsburg* by Derrick Wang. The Report also contains brief background information about the new judges appointed during the two years since the last Circuit Conference, as well as memorial remarks for those who died. The appendices include the actual text of written remarks and other materials referenced during the Conference.

By all accounts, this Conference was a great success. It was attended by more than 750 members of the judiciary, the private Bar, government officials, and guests. I am informed that this attendance was the largest ever at a Second Circuit Judicial Conference. For the most part, this enormous interest and the turnout that the Conference generated can be attributed to two causes: the timely and thought-provoking overarching topic you selected — *Cyber-Security in the Age of Cyber-Terrorism* — and the stellar group of speakers and moderators that the Conference's Program and Planning Committee's various subcommittees were able to recruit to make up the seven expert panel discussions which examined the subject. The comments I received about the substance and quality of the speakers' presentations were uniformly enthusiastic. Such favorable response is a tribute to your outstanding leadership and the huge effort you devoted to ensuring the success of the Conference.

I hope that this Report serves several useful purposes: as an historical record of the Conference; as a substantive source for further review of the subject by the conferees and others; and as a model for future Judicial Conferences in this Circuit and elsewhere.

I thank you again for the honor and privilege you gave me to serve as Chair of the Conference's Program and Planning Committee this year. I look forward to working closely with you on other Court endeavors in the years ahead. I also thank the Committee's co-chairs and members, as well Circuit Executive Karen Greve Milton, Janice Kish, and the rest of the Circuit Court staff, for the extraordinary dedication and diligence they exhibited in this regard. Finally, in connection with this Report, we owe special gratitude to the three rapporteurs who organized and drafted it: Howard Master, Charles Michael, and Harry H. Rimm.

Sincerely,



Victor Marrero

# **Second Circuit Judicial Conference**

## **Report of Proceedings**

### **Table of Contents**

<b>June 12, 2014.....</b>	<b>1</b>
State of the Circuit Report .....	2
Keynote Address: Latest Developments in Homeland Security .....	6
Introduction to Cyber-Crime and Cyber-Terrorism .....	8
Drone Strikes and Targeted Killings: Domestic and International Perspectives .....	11
Cyber-Crime, Cyber-Espionage, Cyber-War, & Cyber-Threats: An Exploration of Illegal Conduct & Warfare in the Cyber-World.....	16
Cyber-War and the Law of Armed Conflict.....	21
Investigating and Prosecuting Terrorism in the Cyber-Age .....	25
<b>June 13, 2014.....</b>	<b>28</b>
Counterterrorism and the Media.....	29
Counterterrorism Technology — the New York City Experience: Privacy and Constitutional Implications.....	33
Report of the 2012-2013 and 2013-2014 Supreme Court Terms.....	37
Dialogue with Justice Ginsburg .....	39
Cyber-Terrorism and the Private Sector: Responses and Liabilities.....	40
Appendix A: Speakers' Biographies.....	48
Appendix B: Remarks of Justice Ginsburg, June 13, 2014 .....	71
Appendix C: Excerpts from Scalia/Ginsburg.....	79
Appendix D: <i>In Memoriam</i> .....	81
Appendix E: Introduction of New Judges .....	82

# **Proceedings**

**JUNE 12, 2014**

## State of the Circuit Report

**Speaker:** Chief Judge Robert A. Katzmann



Chief Judge Robert A. Katzmann opened the 2014 Second Circuit Judicial Conference by welcoming approximately 750 attendees to the Saratoga Hilton in historic Saratoga Springs, New York. After thanking Judge Victor Marrero, Chair of the Judicial Conference, and acknowledging Judge Dennis Jacobs, his “superb predecessor,” Chief Judge Katzmann reported that “the state of the Circuit is good” and provided details on the state of affairs throughout the Circuit’s three states.

*Third Branch Budget:* Chief Judge Katzmann discussed the budget sequester, related challenges to the judiciary’s discharge of the administration of justice and the innovative ways in which the Circuit’s courts were cutting costs. While last year’s sequester, combined with the government shutdown, threatened the judicial system’s ability to continue to provide essential functions, the Chief Judges within the Circuit worked with their court executives to develop contingency plans that allowed the courts to fulfill essential functions and retain employees during the period of strained finances.

Chief Judge Katzmann observed that the passage of the first Congressional appropriations bill in several years provided much-needed financial relief from the prolonged period of fiscal austerity visited upon the federal courts. Chief Judge Katzmann thanked Chief Judge Carol Amon (EDNY), Chief Judge Loretta Preska (SDNY) and Judge Richard Eaton (Court of International Trade) and also praised the Federal Bar Council, the New York State Bar Association, the Federal Bar Association and the New York City Bar Association for making

numerous trips to Capitol Hill to meet with Members of Congress and their staffs to educate Congress about the financial needs of the federal courts in the Circuit. Chief Judge Katzmann noted that Congressional outreach remained a continuing effort because the prospect of severe funding constraints remained as the new federal fiscal year approached.

**New Judges:** Twenty new judges were appointed since the 2012 Judicial Conference. Southern District Judge Richard Sullivan and Eastern District Judge Roslynn Mauskopf were named as Toastmasters to introduce each of the new members of the Second Circuit judicial family.

Chief Judge Katzmann remarked that the quality of the new judges "is simply superb" and thanked the six United States Senators from the Circuit's three states. He extended a cordial welcome to each new judge and wished the judges great distinction and fulfillment in their service to the courts and the nation.

**Judicial Vacancies:** While the Second Circuit had a few vacancies outstanding, the Circuit was "overall . . . in good shape." There are no vacancies on the Court of Appeals. In the District Courts, the Western and Southern Districts of New York have no vacancies at this time. In the four Districts with vacancies — the Eastern District of New York, the Northern District of New York, the District of Connecticut and the District of Vermont — there are judicial search committees working to identify nominees. In Vermont and the Northern District of New York, there are nominees for the vacancies.

In the Bankruptcy Courts, there are three vacancies: two in the Southern District of New York due to the retirement of Judges James Peck and Allan Gropper and one in Connecticut due to the impending retirement of Judge Albert Dabrowski. The Court of Appeals is working to fill these vacancies. Judge Robert Sack chairs the Merit Selection Committee for the Southern District, and Judge Susan Carney will chair the Connecticut Search Committee.

As to Magistrate Judges, there are two vacancies, one each in the Southern and Eastern Districts of New York due to the retirement of Magistrate Judges Michael Dolinger and Robert Levy, both of whom immediately agreed to be recalled and continue to carry full caseloads. The Second Circuit Council has approved these recalls as well as the filling of the Eastern District seat.

**Thurgood Marshall Courthouse:** The Court of Appeals returned to the newly renovated, historic Thurgood Marshall Courthouse (the "Courthouse") after more than six years of displacement. Chief Judge Katzmann noted that since its return, the Court has held a series of lectures, educational programs and receptions to welcome its constituencies into the Courthouse and make it more accessible to the public.

**Public Engagement & Civic Education:** Chief Judge Katzmann noted that it is imperative to find ways in which the Court can bring its constituencies and communities into the Circuit's courthouses to educate them about the justice system, to share ideas for improving the administration of justice in the federal courts, to empower them as citizens to support the federal judiciary and to demonstrate the inherent value of public service in their lives and careers.

Chief Judge Katzmann then outlined a Circuit-wide program of public engagement and civic education designed to bring into the Circuit's courthouses individuals of all ages, backgrounds and experiences by offering innovative and educational programs and events so that they may learn about the work of the federal judiciary and develop a better understanding of the importance of an independent federal judiciary. A few ideas for this initiative were described:

(i) *Young People's Inns of Court*: Chief Judge Katzmann suggested extending the Inns of Court program to "our younger society," including junior high school students, high school students and college students;

(ii) *Evenings at Thurgood Marshall Courthouse*: Chief Judge Katzmann noted his intention to continue hosting evenings at the Courthouse to enable lawyers and non-lawyers to explore the historic Courthouse, visit courtrooms and participate in educational programs;

(iii) *Sharing our Courthouse Space*: Chief Judge Katzmann spoke about sharing the judiciary's spaces with bar associations, civic organizations and student-based groups in need of a place to hold their educational programs;

(iv) *Student Education*: Chief Judge Katzmann proposed sponsoring more organized programs enabling school classes to visit the Courthouse;

(v) *Teacher Institutes*: Chief Judge Katzmann suggested hosting civic teachers and making use of already existing materials to develop modules about the courts which could be part of school curricula; and

(vi) *Court Ambassador Programs*: To assist with staffing the Court's various programs, Chief Judge Katzmann proposed creating a core of senior lawyers to serve as docents, researchers and advisors to the Court's constituencies in the Courthouse. Chief Judge Katzmann invited those who might be interested in serving to contact the Circuit Executive.

Chief Judge Katzmann indicated that he will be creating a new Circuit Committee for Public Engagement and Civic Education with an advisory council comprised of judges, lawyers, educators, academics, curators, architects, engineers, journalists and citizens with an interest in opening the courts to the communities in which the courts are located.

The objectives for this program of civic engagement and public education are to bring communities into the Circuit's courthouses and illustrate for citizens how courthouses are living testaments to the rule of law on which our system depends.

*Hails and Farewells*: Chief Judge Katzmann noted that the Circuit had lost five judges since the 2012 Judicial Conference: Senior Circuit Judge Joseph McLaughlin, Connecticut District Judge Mark Kravitz, Senior Southern District Judge Peter Leisure, Senior Southern District Judge Harold Baer, and Southern District Bankruptcy Judge Burton Lifland.

Chief Judge Katzmann welcomed two new members of the Second Circuit court family appointed since its 2012 Judicial Conference: Gary Gfeller, Clerk of the Connecticut Bankruptcy Court, and Eugene Corcoran, Eastern District Executive.

Chief Judge Katzmann thanked Karen Milton, Janice Kish, Kaleena Guzman, Matt Garaufis, Matvey Zabbi, Larry Sadera, Chris Cooper and Rita Adady for their work in connection with the 2014 Judicial Conference.

Chief Judge Katzmann again thanked Judge Victor Marrero for his extraordinary work as Chair of the 2014 Judicial Conference and expressed his delight that cabinet secretaries, FBI directors, National Security Council officials, academics, a former United States senator, a former Attorney General, military officers, business leaders and media representatives would be participating in the various conference programs.

Chief Judge Katzmann concluded by thanking the members of the Judicial Conference Program and Planning Committee, noting that they had worked hard to develop a spectacular program on cyber-security in an age of cyber-terrorism.



## Keynote Address: Latest Developments in Homeland Security

**Speaker:** Honorable Jeh Johnson, Secretary,  
United States Department of Homeland Security



Secretary Johnson began his address by talking "about what's going on in the Department of Homeland Security" (the "Department"). He noted that the Department has a workforce of 240,000 people and is the third largest department within the federal government. The Department is responsible for the nation's counter-terrorism efforts; the enforcement of immigration laws; aviation, border, maritime and cyber-security; protection of critical infrastructure; protection against biochemical threats; protection of national leaders; and responses to natural disasters.

Secretary Johnson observed that counter-terrorism "is and should continue to be the cornerstone of the Homeland Security mission." He indicated that the terrorist threat against the United States has "changed fundamentally" over the last twelve-and-a-half years because the threat has "morphed," is more decentralized and more diffuse.

One of the Department's concerns relates to the new phenomenon of foreign fighters traveling into Syria and returning to their homelands. Another concern involves the threat of domestic-based terrorists. Aviation security is "vital," and Secretary Johnson has been advocating for what he called overseas preclearance which is a program establishing a Customs and Border Patrol capability and a Transportation Security Agency ("TSA")-like capability in overseas airports that are the last point of departure to the United States.

Secretary Johnson then described an outreach initiative through which the Department partners with community-based groups and state and local law enforcement to address violent extremism in the United States.

Secretary Johnson next spoke about border security. Attempts at illegal border crossings are much lower than they used to be. There has been a recent spike in illegal migration into south Texas, however, by unaccompanied children from Honduras, Guatemala and El Salvador. Secretary Johnson has declared a level four state of readiness within the Department in order to address the problem by, among other things, engagement with the governments of Mexico, El Salvador, Honduras and Guatemala.

Regarding immigration, Secretary Johnson remained optimistic that Congress would undertake comprehensive reform and mentioned that he was undertaking a review of enforcement priorities to ensure that the Department was enforcing immigration laws in a humane manner.

Cyber-security remains a priority for the Department. Secretary Johnson noted that there is renewed interest in cyber-security legislation and offered four areas in need of consideration: (i) clarifying the private sector's authority to share information with the government; (ii) clarifying the Department's authority to obtain cyber-information going to the networks of other parts of the federal government; (iii) limited liability protection for the private sector; and (iv) a data breach notice requirement. Secretary Johnson also observed that he has been meeting with business officials and looking to hire the best talent from graduate schools and universities in order to combat the threat of cyber-attacks.

Secretary Johnson then spoke about the Federal Emergency Management Agency, highlighting how it can rapidly mobilize resources to bring generators, food, water and other supplies into affected areas very quickly and how it can coordinate with state and local government and local communities.

Secretary Johnson commented on the dedicated and professional service rendered by the United States Secret Service. He then spoke generally about management initiatives within the Department, improved morale, strategic approaches to the budget and acquisition processes, and filling Department vacancies.

Secretary Johnson concluded by noting that his job is to preserve American values and to find the right balance between our security and our values.

## Introduction to Cyber-Crime and Cyber-Terrorism

**Speaker:** Michael Bosworth, Special Counsel to the Director of the Federal Bureau of Investigation

What are some of the major types of cyber-crime and cyber-terrorism? How do cyber-criminals and cyber-terrorists inflict harm on others? How is the United States government combating cyber-crime and cyber-terror, and how is it guarding against the risk of a catastrophic cyber-terror attack? These are some of the important issues discussed during Michael Bosworth's lecture.

Mr. Bosworth, a former Assistant United States Attorney for the Southern District of New York ("SDNY"), served as a supervisor for the SDNY's unit investigating and prosecuting cyber-crime before joining the Federal Bureau of Investigation ("FBI"). He used his experiences with the SDNY and the FBI to help the audience understand how cyber-crime works, and how the United States government is fighting it and attempting to strengthen the nation's defenses against cyber-crime and cyber-terrorism.

Mr. Bosworth began his lecture by explaining that, in the words of Director James Comey, cyber-crime is not a "thing," it is a "vector"—a means through which others can harm our businesses, our governments and our personal lives. Criminals and terrorists are using this vector because people are spending increasing amounts of their lives in cyberspace. Mr. Bosworth added that, as Director Comey has stated, the change in the use of vectors "is not something we've seen since the vector change of the early 20th century, when the combination of automobiles and asphalt made it possible for John Dillinger to commit multiple offenses over vast areas in a short period of time."

Mr. Bosworth stated that the cyber-vector takes advantage of the structure of the Internet, which enables computers around the world to communicate with each other via Internet Service Providers ("ISPs"). Computers or computer systems connected to the Internet through ISPs are assigned unique Internet Protocol ("IP") addresses, which may be dynamic (changing over time) or static. Computers communicate over the Internet by contacting other computers, using the IP addresses of those other computers to identify them. Information is then exchanged between computers, identified by their IP addresses, via packets of information that are sent over the Internet between the two devices.

Cyber-criminals and cyber-terrorists differ only in their motives, Mr. Bosworth noted. Both use the open structure of the Internet and similar methods to inflict harm. Mr. Bosworth then described several methods used by both cyber-criminals and cyber-terrorists to harm others. One basic method Mr. Bosworth described is known as "hacking": breaking and entering into a computer system to steal information, spy on the system user or damage the system. The motives of hackers are diverse. Some hackers are fraudsters who are attempting to steal identities or other valuable information for financial gain. Other hackers are state actors who are seeking to gain intelligence on, or to harm, their adversaries. Others are politically-motivated individuals or organizations seeking to make a point.

Mr. Bosworth then discussed another method of cyber-attack: viruses or malware. These are harmful software programs and files that are implanted onto computers, enabling bad actors to damage the infected computers, or to use the infected computers to steal information and harm others. Among other things, explained Mr. Bosworth, infected computers can be employed by bad actors to conduct what is known as Distributed Denial of Service ("DDOS") attacks on intended victims' websites. Mr. Bosworth described how DDOS attackers inflict harm by directing numerous computers under their control to visit a particular website simultaneously, in an attempt to overwhelm the website and force it offline or render it useless. DDOS attacks can be used to make a political point or to mask more harmful hacking occurring at the same time as a DDOS attack.

Other cyber-crime methods summarized by Mr. Bosworth include the publication on the Internet of a victim's private information, a practice known as "doxing," and the use of cyber-tools to generate false reports of emergencies, a practice known as "swatting."

Mr. Bosworth then discussed some of the most serious types of cyber-crimes, including intellectual property theft from governments and businesses, child exploitation and extortion through what is known as "ransomware," which he stated had increased by more than 500 percent over the past year.

Mr. Bosworth cited evidence that cyber-crime targets everyone. He explained that government was a big target because it possesses vast amounts of information, including state secrets and financial information. He cited as an example a recent attack on the South Carolina Department of Revenue in which 3.6 million citizens' Social Security numbers and almost 400,000 debit and credit card numbers were stolen. In addition, businesses of all sizes were targeted.

Mr. Bosworth then addressed efforts by the law enforcement community and the private sector to respond to the growing threat. He described efforts by federal agencies to coordinate efforts and form task forces with state and local authorities to ensure cooperative and effective responses to cyber-crime or cyber-terror incidents. As Mr. Bosworth explained, the FBI and other federal agencies are dedicating significant resources to protecting against and responding to a potential catastrophic cyber-attack by foreign actors, including foreign governments or terrorist groups. He described a 2012 Al-Qaeda video, for example, that "called for electronic jihad against the United States and made a point of equating the vulnerabilities in our nation's cyber-infrastructure with the kind of flaws in aviation security pre-9/11." Mr. Bosworth also highlighted the threat that sophisticated foreign state actors engaged in cyber-attacks posed to the nation. He cited as an example the recent indictment of five members of the Chinese military for hacking and economic espionage offenses that they committed against some of the nation's largest companies over a period of years. He explained that this indictment "was the first time that criminal cyber-charges have been filed against state actors," but "it won't be the last."

Mr. Bosworth informed the audience of significant prosecutions of cyber-crime or cyber-terrorism that were occurring in each of the Second Circuit's judicial districts. He discussed the SDNY's unmasking and prosecution of the creator of the Silk Road online marketplace for illegal drugs and other contraband, which showed cyber-criminals that government has the ability to

track and stop harmful Internet activity that others might have thought was untraceable. The Eastern District of New York, as Mr. Bosworth explained, uncovered and is prosecuting one of the largest coordinated heists of ATM machines in history, enabled by cyber-crime. The District of Connecticut seized and took down servers that controlled a “botnet,” a network of infected computers that were used for DDOS attacks and other harmful cyber-activity, representing the first-ever seizure of its kind. The District of Vermont has led the way in prosecutions of individuals who engage in cyber-crime to facilitate child exploitation, while the Northern and Western Districts of New York have prosecuted novel and significant cases in which cyber-criminals stole valuable intellectual property or marketed counterfeit goods over the Internet.

Mr. Bosworth concluded by discussing the challenges ahead as the nation addresses the growing threat. He stated that while government has made good strides, many questions remained, including what role government should play in coordinating responses to cyber-crime and how to balance cyber-security with privacy interests. While there is a way to protect the cyber-sphere and the rights we cherish, Mr. Bosworth noted, “how to do it at all levels with our international partners,” some of which “may have different norms and standards,” was a challenge that needed to be thought through.

Mr. Bosworth then turned to the role of the private sector and the public in addressing the growing threat. He explained that private sector awareness, coordination and cooperation were critical to combating the cyber-threat, because “all it takes at a company is one bad employee” to compromise network security and enable cyber-criminals to access the company’s network. Mr. Bosworth recommended greater outreach and education efforts to raise awareness of the need for businesses and individuals to practice greater cyber-security, citing recent statistics that 30 percent of people who go online do not even think about cyber-security and that 60 percent of the members of corporate boards of directors either do not know about their company’s cyber-security policy or say that their company does not have one.

Mr. Bosworth concluded by describing several legal and policy challenges posed by the cyber-threat that have yet to be resolved, including Fourth Amendment issues and challenges associated with the potential use of offensive cyber-weapons.



## Drone Strikes and Targeted Killings: Domestic and International Perspectives

**Moderator:** Professor Harold Koh, Yale Law School

**Panelists:** Elisa Massimino, President and CEO, Human Rights First  
Professor Sarah H. Cleveland, Columbia Law School  
Daniel Cahen, Legal Advisor, International Committee of the Red Cross

Does the 2001 law authorizing the use of military force against those responsible for the September 11 attacks allow the United States to use drones against a member of a terrorist group that did not exist on September 11, 2001 (e.g., Al-Shabaab) in a country with no connection to the September 11 attacks and with which the United States is not at war (e.g., Somalia)? Would it make a difference if the target were a United States citizen or if the target were in a car with three civilians? These are some of the difficult questions discussed during the panel.

The panel moderator, Professor Harold Koh, began by raising, and then answering, five "Frequently Asked Questions" targeted to set the stage for further discussion.

First, what is targeting killing, and how does it differ from assassination?

Professor Koh explained that targeted killing is intentional killing by a government or its agents of a combatant who is not in custody, either out of self-defense or because the target is a combatant in an armed conflict. Assassination is murder for religious, ideological, political or emotional gain, and is prohibited by an Executive Order signed by President Ronald Reagan.

Second, what determines whether a drone strike is lawful?

The lawfulness of a drone strike, as Professor Koh explained, breaks down into three issues:

- whether the government's action is consistent with domestic law and international law—an issue which, in turn, is based on both the law of going to war (*jus ad bellum*) and the law of conducting a war (*jus in bello*);
- whether the rights of the targeted person have been adequately considered under domestic and international law; and
- whether the sovereignty of the country where the killing occurred was adequately considered.

Third, what are the relevant bodies of law? As Professor Koh explained, the relevant international law consists of various treaties, including Article 24 of the United Nations ("U.N.") Charter, which contains the general proscription against incursions on sovereignty, Article 51 of the U.N. Charter, which addresses self-defense, and international humanitarian treaties such as the Geneva Conventions of 1949. There also are three bodies of relevant domestic law: (a) the Constitution; (b) statutory law, such as the 2001 Authorization for the Use of Military Force (often

referred to as the “AUMF”);<sup>1</sup> and (c) executive branch policy guidance. Although the executive’s policy guidance is classified, various officials have outlined the broad terms in a series of public speeches.

Fourth, how does this legal framework of domestic and international law apply to the use of drones inside and outside established theaters of armed conflict?

Professor Koh explained that this is a key distinction. The United States is in an armed conflict, under the AUMF, with the Taliban, Al-Qaeda and their associated forces. Drone strikes in Afghanistan and adjacent regions can fall within the law of armed conflict, but the United States has gone further and also asserted, under self-defense principles, the right to use force against senior members of terrorist groups with whom there is no armed conflict.

Fifth, what additional considerations come into play when an American citizen is being targeted?

As Professor Koh explained, the administration has disclaimed the right to target U.S. citizens in the United States, but, outside the United States, the Justice Department has determined that, under certain limited conditions, targeting a U.S. citizen would be lawful. As a result of a Freedom of Information Act suit brought by *The New York Times*, an opinion on this subject from the Office of Legal Counsel is shortly to be made public, at least in part.

Having set the stage with a basic background primer, Professor Koh then asked Professor Sarah Cleveland to address the primary areas of legal disagreement.

Professor Cleveland noted that there are two broad frameworks—the law of armed conflict and the law of self-defense—and pointed to several areas of disagreement.

First, there are difficulties in figuring out the scope of an armed conflict. She asked, “Can you use force, for example, in Yemen or Somalia based on the existence of an armed conflict in Afghanistan?”

Second, there are difficulties in distinguishing belligerents and civilians in an armed conflict. For example, Professor Cleveland asked, “If there’s a car with four people in it and one of the individuals is the person being targeted, how do you think of the other three people in the car?”

Third, the administration’s policy guidance is to use lethal force outside the theater of armed conflict only against persons who pose a continuing imminent threat to U.S. persons, and, as Professor Cleveland explained, the terms “continuing” and “imminent” are subject to debate. A 19th century case called *Caroline*, in which the British forces came into the United States to attack a ship and send it over Niagara Falls, is understood as establishing that it is permissible to enter another country to use force in self-defense where the threat is “instant, overwhelming, and leaving no choice of means, and no moment for deliberation.” The administration,

---

<sup>1</sup> A copy of the AUMF is available at <http://www.law.cornell.edu/background/warpower/sj23.pdf>.

however, has publicly stated that imminence in the terrorism context must be more flexible because terrorist threats are secret and because there may be only limited windows of time in which to target terrorists.<sup>2</sup>

Fourth, Professor Cleveland said there is disagreement about when capture is required. The administration's stated policy is to capture, rather than kill, where "feasible," but it has not given a detailed explanation of what the administration deems feasible.

Fifth, Professor Cleveland raised the concept of "signature strikes," in which the United States targets people not based on knowing who they are, but based on a pattern of behavior. The public knows little about these strikes and about how these strikes fit within the administration's policy guidance.

Finally, Professor Cleveland raised the question of whether the AUMF authorizes drone strikes outside of those aimed at Al-Qaeda or the Taliban. The text of the AUMF refers to the organizations or persons who "planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons." How does this apply to groups such as Al-Qaeda in the Arabian Peninsula or Al-Shabaab, neither of which existed on September 11, 2001? Professor Cleveland said that the administration has claimed that these groups have joined with Al-Qaeda in the fight against the United States and thus should be treated as "co-belligerents."

Professor Koh then turned the discussion to Daniel Cahen to focus on how force may be used — *i.e.*, assuming one has resolved the various issues raised by Professor Cleveland and has concluded that the use of lethal force is lawful. Specifically, Professor Koh asked: How does the United States address civilian casualties, and should victims' families be compensated? He also asked how the United States should address the detention of terrorist suspects.

Mr. Cahen began with some basic background. Under the law of armed conflict, only combatants can be targeted, but there are certain circumstances in which civilians can be lawful collateral damage, including where there is an expectation that an attack with a lawful objective will not result in loss of life or property disproportionate to the expected concrete and direct military advantage. This is "extremely hard to measure in practice," Mr. Cahen said, in part because drone strikes are often in remote locations that are dangerous to access.

Estimates of civilian losses are as high as 30,000, but the true number is difficult to assess, partly because the distinction between combatant and civilian is the subject of debate, Mr. Cahen said. The administration considers people with "sustaining functions" who "help out" terrorist groups to be combatants who can be lawfully targeted, but Mr. Cahen's organization, the International Committee of the Red Cross, believes only those with "more fighting roles" should be considered targetable combatants.

---

<sup>2</sup> A speech on this issue from September 2011 by John O. Brennan, the then-Assistant to the President for Homeland Security and Counterterrorism, is available at <http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an>.

As for the question of accountability, Mr. Cahen said that international and humanitarian law imposes a duty to investigate potential war crimes, but not a general duty to investigate (or compensate victims) every time an attack results in death or lawful collateral damage.

Professor Koh then asked Elisa Massimino: What should the role of courts and Congress be regarding drone strikes?

Ms. Massimino began by saying that she is strongly in favor of targeted killing—as strange as that might sound from a human rights lawyer—because the alternative is not an absence of killing but rather indiscriminate killing. Drone strikes, she added, offer the promise of increased accuracy, which is a good thing from a human rights perspective.

To answer Professor Koh's question, Ms. Massimino said that, although she favors an increased role for federal courts in various areas—including the terrorism trials that are currently happening in Guantanamo Bay, Cuba—she is not in favor of federal court oversight of drone strikes and targeted killing. There are proposals advocating a special court to sanction targeted killings in advance, but those raise separation-of-powers issues and questions as to whether those courts would be improperly rendering advisory opinions. Moreover, she added, the process would appear to be designed to lend a “patina of legitimacy” to executions based on arguments from only one side, and judges, Ms. Massimino said, would be unlikely to want to be involved.

Where the courts should have a larger role, Ms. Massimino said, is to ensure that there is transparency about what our government is doing. On the policy question of what our government should be doing, Ms. Massimino emphasized that there are at least 25 countries with drone technologies and that U.S. policy could shape the way those countries use drone technology going forward.

Professor Koh noted that the next obvious question was: What are the alternatives to drone strikes? He said there are at least four: (1) do nothing, which “seems to be anathema”; (2) a prevention strategy, which involves “winning over the Arab street”; (3) capturing and trying targets in federal court; and (4) capturing and trying targets in military commissions. Professor Koh then turned to questions from the audience.

The first questioner asked: What have been the benefits and detriments of having what the questioner termed a “national security state”?

Professor Koh answered that the question, in some sense, is impossible to answer, but that it is clear there has been a “massive skewing” of government resources towards defense and intelligence. This has produced U.S. intelligence capabilities that are the envy of the world.

Professor Cleveland responded that, as a result of the national security state, courts have been more reluctant over time to oversee the national security activities of the government. She said that the judiciary should be more mindful that it is a co-equal branch that plays an important role in balancing security against individual rights.

Another questioner asked: What difference does it make, from a legal perspective, as to whether a target is a U.S. citizen or not, given that the Due Process Clause of the Constitution refers to persons, not citizens?

Professor Koh answered that several courts have ruled that aliens who have never entered the United States do not have due process rights, thus appearing to recognize the distinction. Professor Cleveland added that, while she agreed with Professor Koh that courts have made such a distinction, she found it to be an "awkward" one. If a person is lawfully the target of lethal force, it should not make a difference if that person is a U.S. citizen or not.

The final audience questioner said that he generally understood that participants in war should do whatever is necessary to win the war and that shortening the war can reduce casualties overall. He asked about specific examples where one side has used force apparently directed at civilians — when England bombed Cologne and when the United States firebombed Tokyo. He then raised a final, unrelated issue, of whether it would be appropriate to use drones in Somalia to attack terrorists who have kidnapped hundreds of innocent schoolchildren, notwithstanding that we are not at war with Somalia.

Professor Koh said that, along the lines of the bombing examples, the United States used nuclear weapons in World War II, which led to the U.N. Charter and the Geneva Conventions.

As for the example of the kidnapped schoolchildren, Professor Koh said its lawfulness would depend on whether the kidnappers were considered "co-belligerents" with Al-Qaeda or the Taliban — a question he could not answer. Mr. Cahen added that, if the host government consented, however, there might be lawful grounds to target the kidnappers.



## Cyber-Crime, Cyber-Espionage, Cyber-War, & Cyber-Threats: An Exploration of Illegal Conduct & Warfare in the Cyber-World

**Moderator:** Honorable Preet Bharara, United States Attorney,  
Southern District of New York

**Panelists:** Honorable Robert S. Mueller, III, Wilmer Cutler Pickering Hale and Dorr LLP  
Honorable Michael Chertoff, The Chertoff Group  
Edward M. Stroz, Stroz Friedberg LLC



What are the most significant threats facing the United States as a result of the growth of cyber-crime and related illegal conduct occurring over the Internet? What are governments and the private sector doing to combat the growing threats, and are those efforts sufficient? What are some of the policy and philosophical considerations that should influence our evaluation of efforts to regulate and combat illegal conduct occurring in the cyber-world? These are some of the important issues discussed during the panel discussion, which is summarized below.

Mr. Preet Bharara began the panel discussion by asking the panelists which cyber-threats concerned them the most and which cyber-threats they believed the nation was least prepared to address. Director Robert S. Mueller who served as United States Attorney for the Northern District of California, Assistant Attorney General and Director of the FBI before entering into private practice, asserted that the greatest cyber-threats are to financial institutions and exchanges, followed by threats to infrastructure such as the power grid. Director Mueller stated that the threat to financial institutions is more severe than the threat to infrastructure because financial institutions and exchanges already are on the Internet and are thereby exposed to cyber-threats that could harm not only the institutions and exchanges, but the economic capability of the United States. Infrastructure, by contrast, is less exposed to the Internet.

Secretary Michael Chertoff, who previously served as Secretary of the Department of Homeland Security ("DHS") and Circuit Judge for the United States Court of Appeals for the Third Circuit, agreed with Director Mueller and added that the greatest cyber-threats to national security are those that would allow the United States' enemies to use technology not only to steal information, but to access and damage control systems that affect real-world activities, including air traffic control systems, systems that operate markets or even airplanes, automobiles or other machines that could be accessed and controlled remotely. Mr. Edward M. Stroz, a former FBI Supervisory Special Agent who founded and serves as Executive Chairman of investigative firm Stroz Friedberg, joined in the other panelists' assessments and asserted that risk management principles need to be applied to cyber-threats to ensure that the nation is prepared to address the most severe risks to national security.

Mr. Bharara next asked the panelists whether the government had the ability to recruit and retain people who were smart enough and cutting-edge enough to deal with the cyber-threat, and further whether the government had the resources to combat the threat effectively. Secretary Chertoff contended that the government is moderately successful at attracting top talent, in spite of the inability to pay top talent at levels commensurate with those in the private sector, because it benefits from the ability to draw individuals attracted to the cutting-edge technology problems handled by the National Security Agency and other government agencies. Secretary Chertoff added, however, that most infrastructure is in private hands, thus rendering the government unable to protect that infrastructure directly. He also noted that regulation has been ineffective at securing private sector infrastructure. There is a need, according to Secretary Chertoff, for a new framework that would enable people to share information on cyber-threats without the fear that the information would become public or that people making disclosures would be exposed to liability. There also is a need for a well-developed doctrine and appropriate legal authorities to permit the government to take appropriate steps if a destructive attack occurs and there is a need for the government to be involved directly.

Responding to Mr. Bharara's question concerning the government's ability to hire top talent, Director Mueller stated that the FBI and other federal agencies involved in addressing cyber-threats are able to draw top talent that is able to combat the cyber-threat not only with technical skills but also with the ability to investigate cases using traditional investigative techniques applied to the cyber-area. Mr. Stroz echoed that sentiment, noting that FBI agents have unique abilities to investigate and solve crimes, giving them an advantage when compared to private sector cyber-industry talent without that experience.

Mr. Bharara then asked whether the panelists agreed that the private sector shared responsibility for cyber-security or whether the government was responsible for cyber-security as part of its obligation to provide for "the common defense," in the words of a cyber-security executive. Mr. Stroz replied that the private sector has to play a role in protecting its own property. Mr. Bharara then asked whether private sector entities that are under attack from cyber-threats are doing enough to coordinate their efforts with each other and the government. He used the analogy of a bank robbery to make the point: "In the old days you would never imagine that a financial institution after being robbed at gunpoint by a person with a mask wouldn't immediately call the police or FBI or whoever and report that. And yet often it's the

case in real life experiences that financial institutions are basically the victims of a similar kind of bank heist or robbery and they're delaying days, weeks and sometimes never ever disclose to law enforcement. How big a problem is that and why is that?"

Secretary Chertoff responded that the problem identified by Mr. Bharara used to be bigger, but is improving. He noted that the private sector has to play a role in thwarting and responding to cyber-attacks because the backbone of the internet "is not in the military, not in the government, but is with the private sector." He reiterated his earlier claim that a mechanism is needed for private sector actors to provide intelligence on cyber-threats to the federal government and for federal government agencies to disseminate intelligence to the private sector so that it can respond to cyber-threats more effectively. Mr. Bharara asked what incentive private sector actors have to cooperate with government, given the intrusion of privacy and risk of harm to the company's reputation or its stock price if a cyber-attack is reported to the government and publicized. He asked why private sector actors should not just respond to cyber-threats on their own and "hope that the next guy that gets attacked is their competitor?"

Secretary Chertoff replied that "everybody gets attacked" and that therefore the shame and embarrassment of being attacked by cyber-criminals was diminishing. He also noted that private sector actors are realizing that, as a matter of self-interest, cooperative exchanges of information actually could reduce the risk for everybody. He noted that banks do not want to compete on the issue of cyber-security, much as airlines do not want to compete on the issue of safety, because it was not in their interests to have consumers thinking about cyber-security when banking. He added that it is in the private sector's interest to beef up cyber-security to avoid a scenario in which the government has to monitor a company's activities to guard against and respond to cyber-threats.

Mr. Stroz stated that there are reasons for delayed reporting and responses, both by the government and the private sector. He stated that sometimes the government can delay responses to cyber-threats as it attempts to investigate and apprehend the perpetrators of cyber-attacks. He also raised the concern that, in many cases, cyber-attacks are stealthy, and the only individuals in a position to detect attacks—employees of company IT departments—are the same individuals who stand to get in trouble for reporting those attacks. He noted that this potential conflict of interest may cause delays in reporting and that the threats need to be managed more effectively to avoid delays or problems in reporting in the future.

Mr. Bharara then asked whether the culture of sharing information in order to increase safety found in the airline industry, referenced earlier by Secretary Chertoff, is found in the private sector in dealing with cyber-threats. Director Mueller stated that Silicon Valley's competitive environment provides disincentives for cooperation. Secretary Chertoff argued that, while the private sector needs to do a better job of cooperation, the government also needs to "share back." He noted that sometimes the government will receive a report of a cyber-attack from the private sector, and the government's only response will be to say "thank you." He stated, "I think there's got to be a certain amount of mutuality" so that private sector actors running critical infrastructure "get the benefit of some of what the government knows." Director Mueller responded that information-sharing is in fact happening. He cited statistics

indicating that, in 2013, about 3,000 entities were informed by either the FBI or DHS that their networks had been compromised, principally by Chinese actors. Fully 70 percent of those notified did not realize that their networks had been compromised. Mr. Stroz noted that in some cases, it may be helpful to victims of cyber-attacks for the victims or law enforcement to monitor attackers before taking steps to stop the attack in order to avoid bigger problems. He gave as an example situations in which a client wanted to change passwords immediately upon detection of a threat. He stated that he would advise clients in those circumstances not to do so because, "if you do that, A, they're going to know you're inside, and B, they're going to get all the changed passwords."

Mr. Bharara then turned to the question of what roles various government agencies play in preventing and responding to cyber-attacks and whether lines of responsibility were clear. Both Director Mueller and Secretary Chertoff stated that, when serving in their roles as heads of the FBI and DHS, respectively, they worked diligently with each other and with other federal agencies to delineate clearly the various lines of responsibility. They noted that while turf fights might arise on occasion, there is "plenty of work to go around."

Mr. Bharara then asked the panel to address the cyber-threat posed by foreign nations, in particular China. He asked the panelists whether responses to the Chinese cyber-threat are being affected by "narrow self-interest," in which companies are engaging in a "cost-benefit analysis," essentially balancing the financial benefits of accessing the Chinese market against the costs of the theft through cyber-crime that inevitably will occur in China. Secretary Chertoff stated that there was a "wide variety of views on the issue of China" in the private sector. He agreed that some companies were conducting a cost-benefit analysis of the type described by Mr. Bharara, but added that one of the factors some companies consider is that technological secrets stolen in China may not be usable by Chinese companies until the technology has already been rendered outmoded by ongoing research and development efforts outside of China. Secretary Chertoff also added that Russia posed a significant cyber-threat.

Mr. Bharara asked the panel whether it ever makes sense for a company to take matters into its own hands by engaging in offensive actions, known as "hack backs," against individuals or entities believed to be engaging in cyber-attacks against the company. Mr. Stroz explained his view that the idea was unwise because, among other things, it is difficult for a private company to know the true origin of a cyber-attack. Thus, a hack back presents the risk that an offensive action may target the wrong individual or entity.

Mr. Bharara then asked whether the response to cyber-threats had become too complicated, and whether the most important steps to combat such threats were actually simple, much as the best way to combat infection in hospitals turned out to be a simple one: washing hands. Mr. Stroz agreed, stating that "the simple things go a long way to making it better," including protecting passwords, keeping systems patched with the latest security updates and ensuring that all participants on conference calls are fully identified.

Mr. Bharara concluded the panel discussion by asking whether, in cyber-space, there remained any "pure space for anonymity that is appropriate that law enforcement and intelligence services shouldn't be able to touch?" Secretary Chertoff replied that the question

should be broken up into two parts: first, "should the government be able to build the capability, the potential to elicit or intercept" cyber-communications, and second, "under what circumstances should it have the authority to exercise it?" He said that the answer to the first question was straightforward: the government should be able to build the capability to get into any network, "assuming that it has the legal authority and appropriate permission to do so," with the caveat that, in his personal view, the government should not "make it easier for itself by weakening the overall structure of security for widely distributed products." Secretary Chertoff also contended that privacy interests and security interests are not mutually incompatible, stating: "You can't have privacy without security." Director Mueller joined with Secretary Chertoff in stating that it was essential to national security that the government be able, with appropriate authorization, to access cyber-communications in order to avoid having increasing portions of the Internet "go dark." Mr. Stroz added that, while everyone should have the right to anonymity, it is important to be able to combat criminal operations such as Silk Road that take advantage of anonymity to facilitate crimes.

Mr. Bharara then opened the floor to questions. One audience member asked when a cyber-attack is "big enough" to be reported to law enforcement. Mr. Stroz stated that, while some crimes might be too small to prosecute on their own, "a minor event can be one little tentacle of a much bigger problem," thus calling for some attention to determine whether the reported issue is indicative of a bigger issue that may warrant law enforcement support. Director Mueller stated that the increasing frequency of cyber-attacks at companies such as Target increases public awareness of the necessity of addressing the problem in new and different ways. Mr. Bharara asked whether the Target cyber-attack, which resulted in the termination of the company's CEO, had affected how people in the private sector think about the cyber-threat. Secretary Chertoff responded that it had by raising consciousness about how to respond to cyber-attacks and the risks and costs of failing to address them.

A second audience member stated that the panel's discussion of the cyber-threat to the electric grid was terrifying, and asked whether more could be done to address the threat. Secretary Chertoff responded that, according to surveys, the electric utility industry was one of the industries that was best prepared to respond to the cyber-threat and that because the industry is regulated, utilities already have redundancy and resiliency built into their systems to address cyber-attacks.

A third audience member asked whether the panelists would support tort liability for third-party security software providers or government indemnification of private companies that comply with potential new legislatively-imposed duties in responding to the cyber-threat. Secretary Chertoff stated that he does not support expansion of tort liability, and both Secretary Chertoff and Director Mueller stated their support for "safe harbors," or limitation of liability, for companies that create security tools or provide information to the government to combat the cyber-threat.

## Cyber-War and the Law of Armed Conflict

**Moderator:** Professor Samuel Rascoff, New York University School of Law

**Panelists:** Professor Harold Koh, Yale Law School  
Professor Matthew Waxman, Columbia Law School  
Professor Ashley Deeks, University of Virginia Law School  
Colonel Gary Brown (Ret.), International Committee of the Red Cross



This panel explored how and whether laws and norms developed based on conventional warfare should apply to cyber-attacks—attacks that may cause substantial, tangible harm but do not resemble a typical act of war like dropping a bomb. Complicating matters further is the difficulty of developing new laws and norms in an area that is inherently secretive: cyber-attackers do not announce who they are and the victims may not want to admit having been vulnerable.

Professor Samuel Rascoff began the discussion by distinguishing cyber-warfare from other conduct in cyberspace. Perhaps the only publicly known instance of cyber-warfare, he said, is the "Stuxnet" worm, which was jointly created by Israel and the United States and which damaged 1,000 centrifuges in an Iranian nuclear facility. By comparison, in 2012, Iran initiated a cyber-attack that allegedly damaged 30,000 computers at the Saudi oil company Aramco but did not directly impact Aramco's physical infrastructure. Somewhere between the Stuxnet attack and the Aramco attack, Professor Rascoff said, likely lies the important distinction between what is and what is not an act of war.

Professor Rascoff suggested framing the conversation by comparing the strategic, policy and legal questions to those that were facing the world on the eve of the Cold War, when the prospect of nuclear war was reshaping power and reshaping the law. This comparison can be seen in three ways.

First, cyber-war raises strategic questions: Who will be using these cyber-weapons, and how will they be used? Will they be used strategically the way that nuclear weapons have been as a way of shaping or reshaping the global balance of power? Will they be used tactically or operationally in conjunction with traditional conventional nuclear weaponry? What would escalation look like in cyberspace? What does deterrence look like in cyberspace?"

Second, cyber-war raises questions about what institutions will be relevant. The United States has taken the lead in this area, as it did during the Cold War. The key institution is the U.S. Cyber Command, which is co-located with the NSA and which operates mainly in cyberspace.

Third, cyber-war raises legal questions: What counts or what ought to count as a use of force within the meaning of the *jus ad bellum* (the law of going to war) in international law for purposes of cyber-warfare? Should it be a test about breaking things and killing people in the world or should it be some other kind of test? When is an act of self-defense justified in connection with cyber-warfare?

Before turning to the panel, Professor Rascoff raised two complicating factors that distinguish cyber-war from nuclear war—secrecy and attribution. Whereas there was a mushroom cloud over Hiroshima and Nagasaki, there is no such equivalent in cyberspace. Stuxnet became public only because the virus accidentally migrated outside Iran. And even if the cyber-attack becomes known, it is often unclear who has initiated it.

Professor Rascoff turned the discussion first to Professor Harold Koh, who was most recently the State Department's Legal Adviser and who published a speech about the application of the law of armed conflict to cyberspace.<sup>3</sup> Professor Rascoff asked Professor Koh whether there has been a new norm applying the law of armed conflict to cyberspace, and what challenging issues have arisen.

Professor Koh responded with some of the key themes of his published speech. At the outset, he echoed Professor Rascoff's point that cyber-war is only one of many activities in cyberspace. There can be all manner of cyber-intrusions, such as cyber-espionage, but those intrusions can, in a manner of minutes, turn into an attack. While there is a clear conceptual difference between exploiting a computer network and attacking it, the difference is "virtually meaningless" in practice because countries and companies have to respond to both.

Professor Koh next said that the United States has made clear that cyberspace is not a "law-free" zone and that the laws of war do apply to cyber-war. It is self-evident, he said, that causing a hospital to lose electricity and thereby causing people to die is no different from dropping a bomb. The harder questions arise when the physical harm is less manifest.

Other principles of the law of war apply to cyberspace, including the law of conducting a war (*jus in bello*). For example, it is unlawful to attack civilians or respond disproportionately.

---

<sup>3</sup> A copy of the speech is available at <http://www.state.gov/s/l/releases/remarks/197924.htm>.

But these principles can be tricky in cyberspace because of the need for swift countermeasures. "Something that looks like a response in self-defense can quickly become something that looks offensive," Professor Koh said.

Further, the line between civilian and military is less clear in cyberspace because there is often "dual use" infrastructure, such as servers. An attack on a server could damage business infrastructure and thus be considered an attack on civilians.

Professor Koh raised a final question of what institutions should govern in cyberspace. One alternative is to do nothing. Another model would be a state-to-state model in which countries negotiate treaties, but the problem with that model is that cyberspace has traditionally had other stakeholders, including private business.

Professor Rascoff then turned the discussion to Colonel Gary Brown, the first Legal Adviser to the U.S. Cyber Command. Professor Rascoff highlighted a dilemma from Professor Koh's remarks: How do we draw a clean distinction between espionage (which is not regulated) and cyber-war (which, it is generally agreed, should be) when, as Professor Koh pointed out, the difference between the two "can be vanishingly hard to tell?"

Colonel Brown conceded that the question raised a dilemma. He underscored the point with the following illustration: "If you cut the wire around a base and walk on to a base it isn't immediately clear whether or not you might be a saboteur or a spy. The problem in cyberspace is you can change from one to the other in milliseconds and engage in very, very significant espionage very rapidly or you could flip the switch and go the other way and destroy the entire system before it has a chance to respond."

Professor Rascoff then turned the discussion to Professor Ashley Deeks, who has published extensively on cyber-warfare and who previously served as Deputy Legal Adviser of the State Department. He asked how she expected law to be made in this area and to comment on the role that secrecy would play in creating law for cyber-attacks.

Professor Deeks began by saying that there is a general consensus that the law of armed conflict can apply to cyber-attacks if, for example, it resulted in the same kind of harm as "kinetic activity." She said it was not even clear Stuxnet would meet that standard.

Professor Deeks added that states are giving consideration to how various other legal norms can be translated into cyberspace, as well. For example, there are norms providing that (a) a state should have the right to control activities within its territory (territorial sovereignty), (b) states should not excessively interfere in another state's economic, social and political activities (non-intervention) and (c) states should not allow conduct within their territory to spill over and harm neighboring states. The content of these norms is heavily debated—"squishy"—and states are trying to figure out how they apply to cyberspace.

As for the future of making law in this area, Professor Deeks said that international law generally comes in two forms: treaties and customary international law. She said it would be hard to imagine formal treaties in these areas because states do not want to reveal what they are doing. She expected the developments to occur primarily through state practice.

Returning to Professor Rascoff's question about secrecy, Professor Deeks said that states are unlikely to say what they have done and why regarding cyber-attacks. Rather, she expects that international norms will form when there are unauthorized leaks, and when governments are forced to defend what they have done, or norms may develop when states forced to defend against cyber-attacks themselves must explain who attacked them and why those attacks merit a response.

The discussion then turned to Professor Matthew Waxman, who like Professor Deeks, has published extensively on these issues. Professor Waxman also held various government positions in the White House, the State Department and the Pentagon earlier in his career. Professor Rascoff asked Professor Waxman about how the issues discussed would manifest themselves in domestic law and before U.S. courts.

Professor Waxman said that the U.S. government's involvement in an attack, or in defense of an attack, could involve seizing or blocking data or communications in ways that raise property, privacy or free speech issues. This could raise questions about what is justiciable and what degree of deference the courts will give to the government. Should it be the same extensive deference given to the government concerning conventional war?

Generally, there is more deference given to the executive in foreign operations, but, Professor Waxman said, the line between domestic and foreign in cyberspace is a "blurry one." The level of deference would also likely depend on how closely the conduct resembles traditional military conduct. The closer the resemblance, the more likely the courts would defer to the executive, Professor Waxman said.



## Investigating and Prosecuting Terrorism in the Cyber-Age

**Moderator:** Honorable Loretta E. Lynch, United States Attorney,  
Eastern District of New York

**Panelists:** Honorable Joseph I. Lieberman, Kasowitz, Benson, Torres & Friedman LLP  
Honorable Michael Chertoff, The Chertoff Group  
Honorable Michael B. Mukasey, Debevoise & Plimpton LLP



The Honorable Loretta E. Lynch, United States Attorney for the Eastern District of New York, introduced a panel formed to discuss the challenges associated with investigating and prosecuting cyber-terrorism in the cyber-age.

Ms. Lynch asked former United States Senator Joseph I. Lieberman to discuss how the threat of cyber-terrorism compared with more traditional types of terrorism. Senator Lieberman observed that the focus previously has been on Islamist extremist terrorism and threats to infrastructure from terrorist physical attacks. With the creation of the Department of Homeland Security ("DHS"), the new agency worked together with the Director of National Intelligence and the National Counterterrorism Center to coordinate a response to the threat of cyber-terrorism.

Ms. Lynch then asked former DHS Secretary Michael Chertoff whether he viewed cyber-tools primarily as a means of preventing terrorism or just as a means of protecting our cyber-infrastructure. Secretary Chertoff focused on two ways in which cyber-issues came to the fore within DHS. First, cyber-tools were and are significant to the recruitment and training of people, and in communications related to, and the execution of, terrorist plots. Second, cyber-infrastructure became an attractive target for terrorism, in response to which the government established a comprehensive national cyber-security initiative. Secretary Chertoff also stated that the domestic faces of cyber-security are the domestic civilian agencies, like the DHS and FBI.

Former Attorney General and former United States District Court Chief Judge Michael B. Mukasey then discussed the creation of the National Security Division of the Department of Justice. Judge Mukasey said it "was enormously helpful" because of the cooperation among participants. He said rules were implemented to turn the FBI into an intelligence gathering agency, in addition to being a law enforcement agency. While noting that terrorists traditionally were known for killings on as large a scale as possible, Judge Mukasey predicted an increase in the use of "cyber" both in recruiting and as an adjunct to future attacks.

Ms. Lynch next questioned whether cyber was a weapon or simply a means. Secretary Chertoff suggested that, over time, cyber would likely move from becoming an enabler of physical terrorism to an end attack of terrorism, noting that "smart devices" could easily become "attack vectors," with real world consequences. Senator Lieberman observed an inevitability to terrorist groups becoming more sophisticated and using cyber as a form of attack on our country's infrastructure, which he pointed out is managed by cyber — our electrical grid, water systems, financial systems and communications systems. Secretary Chertoff added that, increasingly, cyber was being used as a weapon by groups for ideological, political and other reasons.

The panelists then discussed whether cyber-security strategy would allow for the internet, or certain websites, to be shut down. Judge Mukasey said that we have the capacity to do it and that he believed that the government had the right to do it if it wished to do so. Senator Lieberman said that legislation to provide the President with the authority to close down the internet nationally or in a specific region was opposed. He further explained that cooperation from the private sector is vital because most of the country's critical infrastructure is privately owned and controlled and that the private sector strongly opposed comprehensive cyber-defense legislation due to government regulation. The private sector simply has to be better at creating defenses.

Ms. Lynch asked how we can push the private sector to do more. Secretary Chertoff offered several recommendations, including establishing liability protection for companies that raise the standard for their protection to a reasonable level of performance standards, and translating technical jargon related to cyber-security into simpler language that senior executives can understand so that it can be acted upon more effectively.

Ms. Lynch next inquired as to what can be done to expand or manage ".com" companies. Judge Mukasey said that companies should get together and consult with those sharing technical capability in order to protect their secrets and maintain a level of security that the companies cannot handle by themselves. Senator Lieberman remarked that cyber-defense is an area that really calls for a public/private cooperation and partnership.

The panelists then considered whether the fallout from Edward Snowden's disclosure of confidential government files would likely dampen information sharing that could be a vital tool to security protection. Senator Lieberman answered affirmatively, but cautioned that such a response is "totally irrational and unconnected." Secretary Chertoff explained that Snowden has had a "tremendously damaging impact" on our ability to protect ourselves with respect to cyber. Companies in the private sector are scared to cooperate with the government, and

allies are placed in a position where they are concerned and afraid that "they're going to be outed." Judge Mukasey concluded by alluding to panic among allies, private business and Congress.

Ms. Lynch next inquired about other governmental responses (other than legislative) that might help in protecting us from terrorists using cyber and pure cyber-infrastructure issues. Senator Lieberman explained that President Obama acted wisely by issuing an Executive Order to develop a process allowing the government and private sector to work toward developing certain standards to defend. He also added that "reality has begun to awaken companies" and that companies are now spending more money to defend against cyber-attacks and cyber-crime. Secretary Chertoff noted that we can educate people about what they ought to do even if we cannot provide a direct incentive and that basic education would allow companies to understand the threat and how to conduct themselves on the internet.

The discussion then turned to whether the Department of Justice has what it needs to keep up with the cyber-threat in terms of being able to share information and work cooperatively. Judge Mukasey noted that the Department of Justice cooperates with local authorities on a regular basis. He added that it would be prudent to focus on education and educating people about the nature of what the government collects, what it does not collect and why it collects it.

Ms. Lynch next asked if there was a disconnect with the citizenry in terms of how people view their own cyber-security and what we do about that issue. In response, Messrs. Chertoff, Lieberman and Mukasey focused on the wealth of commercial data that is collected by and held in private hands and then used and marketed with minimal constraints.

Ms. Lynch concluded by inquiring what each panelist might want from a wish list in order to provide better cyber-security or combat cyber-terrorism. Senator Lieberman suggested passing cyber-security legislation, including offering immunity from liability to privately-owned infrastructure if the companies prove that they have met or attempted to meet certain standards. He also suggested authorizing — by statute — cooperation or the sharing of information between the government and private entities and among private entities. Secretary Chertoff explained that the focus should be on better allocation of responsibility between domestic and military agencies as to threats which are "away and home." Judge Mukasey sought a revised authorization for the use of military force.

Following the panel discussion, two comments were raised by the audience. First, a concern was raised about the need to focus on the individual, not just the technology. Secretary Chertoff agreed that it was critical to focus on people who present risks while balancing that with civil liberties. Senator Lieberman focused on the increasing problem with so-called lone wolves who operate on their own. Second, a concern was raised about not letting the government "off the hook" and requiring government to raise its standards to protect itself better. Judge Mukasey agreed that government should be able to do a better job. Secretary Chertoff concluded the panel discussion by observing that the government needed more effective ways of monitoring its own networks for problematic behaviors and suggested assembling a group to take a thorough look at the way counter-intelligence is being managed.

# **Proceedings**

**JUNE 13, 2014**

## Counterterrorism and the Media

**Moderator:** Carol Heckman, Harter Secrest & Emery LLP

**Panelists:** Dina Temple-Raston, National Public Radio  
Barton Gellman, Journalist  
Randy L. Shapiro, Global Media Counsel, Bloomberg LP  
Honorable William J. Hochul, Jr., United States Attorney, Western District of New York



This panel explored the sometimes difficult balance between secrecy and accountability and featured topical insights on these issues from a federal prosecutor, a media lawyer and two reporters. Carol Heckman, a former federal magistrate judge and now an attorney in private practice, served as moderator. She began the discussion with a simple, direct question to the Honorable William J. Hochul, Jr.: How do you balance the public's right to know with the need for secrecy in prosecutions involving classified information?

Mr. Hochul began by pointing out that disclosure in terrorism cases is sometimes desirable. For example, in the case of the "Lackawanna Six" involving six Yemeni-Americans convicted for having attended Al-Qaeda training camps in Afghanistan, the community itself provided key initial leads. He added that the prosecutors in the Western District of New York consider the press as a partner and have a strong relationship with the local media.

Ms. Heckman then turned to the reporters on the panel to ask a related question: "Are you satisfied with letting the prosecutors decide what classified information or what sensitive information gets out to the public when there's a prosecution of this nature?"

Barton Gellman, a reporter perhaps best known for having been among the three journalists who received and reported on information directly from former National Security

Agency contractor Edward Snowden, responded that he considers information designated "classified" by the government to be a "yellow light, not a red light" in his reporting. Security requires some measure of secrecy, he said, but secrecy "often is in tension with the fundamental ideas of self-government." Mr. Gellman said that there were extensive materials from Mr. Snowden that he never had any intention to publish and that he took extensive measures to keep the information secure.

Dina Temple-Raston added that she considers it her job to reveal when the government is doing something wrong. She gave an example of having reported on FBI training materials that were offensive to Muslims. This was important information to disclose, and it resulted in changes in FBI training.

Ms. Heckman asked Mr. Hochul about the process that the U.S. Attorney's Office employs when it learns that the media has information relevant to an investigation.

Mr. Hochul said that the first step would be to attempt to get voluntary cooperation. He mentioned a domestic terrorism case in which a *Buffalo News* reporter was able to interview the defendant, who made several admissions. The reporter was willing to testify in multiple proceedings. If the government cannot get voluntary cooperation, there is a new, cumbersome procedure that requires the personal approval of the Attorney General of the United States before issuing compulsory process to a reporter.

Ms. Temple-Raston noted that it is important for journalists not to be part of the story and asked Randy Shapiro whether she would have advised the *Buffalo News* journalist to testify. Ms. Shapiro said that Bloomberg LP has a policy about not reporting on itself, but that having a reporter testify about being a witness to a crime is not *per se* a problem. She said, however, there is a slippery slope that arises when the questions involve discussions with sources. Bloomberg LP will sometimes allow a reporter to submit an affidavit repeating under oath what has been published in a news story, but generally will not go any further.

Mr. Gellman added that there is an important concern in these situations that reporters not be viewed by the public as arms of the government because that can impair the public's trust in the role of the press as a watchdog over the government.

Ms. Heckman then turned back to Mr. Gellman's reporting on Edward Snowden and asked him to discuss his process for dealing with classified information. Mr. Gellman said he has extensive experience reporting on national security and classified matters. He starts with the proposition that, in the context of foreign policy or national defense, anything that is not in a press conference or news release has probably been deemed "classified" by the government. It is also important to recognize, Mr. Gellman said, that so-called "classified" information is routinely leaked deliberately so as to advance the agenda of the leakers. These types of leaks are usually authorized by political appointees or other top officials.

What Mr. Gellman found with Mr. Snowden, however, was not the typical leak of a government official promoting a government agenda. It was top secret material that was highly compartmentalized even within the government, and Mr. Gellman knew immediately that there was much information he would never reveal publicly.

The first story that Mr. Gellman published involved PowerPoint slides showing how the government obtained substantial information from internet service providers under Section 702 of the Foreign Intelligence Surveillance Act. The program was called “Prism.” Mr. Gellman reached out to three government officials and asked them to find the PowerPoint document on their own, and then to call him back to discuss. He started the conversations by conceding that certain operational information — essentially how bad guys were caught — would never be published. In the course of the discussions, he and the government agreed as to what else would be too sensitive to publish, with one exception. The government did not want Mr. Gellman to publish the names of the companies participating in the Prism program out of concern that they would be less likely to cooperate in the future. Mr. Gellman responded: “That we cannot accept as a valid harm, that the public will react wrongly and try to direct you and the company differently by the way that they vote with their dollars and their votes. That’s not harm we can accept as a reason not to publish.”

Ms. Heckman then asked Ms. Temple-Raston how she balances the competing issues of secrecy and the public’s right to know, and also why the journalist, rather than the government, should be the one to decide.

Ms. Temple-Raston said that there is a common misperception that journalists are motivated primarily by getting “scoops,” when in fact they often work closely with the government to strike the right balance. She gave an example from her investigation of a story relating to Somali-Americans in Minneapolis traveling back to Somalia to join the terrorist group Al-Shabaab. Ms. Temple-Raston visited a hookah bar and was chatting with high school students who described how they were recruited to travel to Somalia to join Al-Shabaab. When she approached the FBI with the information she learned, the FBI said it was in the middle of an ongoing investigation that would be compromised by a media story. NPR and the FBI eventually agreed that NPR would write various parts of the story prior to the arrests and save other parts for after the arrests.

Mr. Gellman then addressed the second part of Ms. Heckman’s question — who elected the journalist to make these decisions? He said that there has to be a role for the press because of the government’s fundamental conflict of interest: government officials cannot use their power to affect the public, while at the same time deciding how much information the public ought to have in holding those officials accountable for that use of power.

By way of example, Mr. Gellman said he has in his possession, and has reported on, the entire secret intelligence budget (the so-called “black budget”) for the prior fiscal year. He told the Director of National Intelligence that, from these thousands of pages, he was going to publish about 25, with redactions. The Director had no objection. Mr. Gellman noted that someone had made the decision within the government that all of this information — even the top line numbers — should be marked classified, but then did not actually object to its publication and never claimed that any harm flowed from its publication.

Mr. Gellman added that another key element to the discussion was that the government is not only over-classifying matters, but is also often deceiving the public. He said: “There are times the U.S. government behaves as though it accepts Churchill’s famous wartime dictum that

in war times secrets are so precious they need to be attended by a bodyguard of lies." One example was Section 215 of the Patriot Act, which authorized the government secretly to request business records and other tangible things relevant to terrorism investigations. The discussion around its passage concerned the risk the government would abuse the authority to find out private information by serving, for example, requests on libraries to find out what people were reading. The government assured the public that the Section 215 tool was limited. In 2009, the government said that it had used Section 215 only 21 times. That was about the only thing known about the use of Section 215, so it appeared that concerns about its abuse were unfounded. But thanks to what Mr. Snowden's materials have revealed — and only from those disclosures — we know that 12 of those 21 orders allowed the government to obtain substantially all the phone call records of all Americans.

Mr. Gellman gave one further example of how secrecy reduces accountability. He published a story in August 2013 about an internal National Security Agency accounting of its compliance with its own rules. The top level numbers, just the number of incidents, were marked "secret," which is a very low level of classification for the government. When the identical table was given to Congress, however, it was given a substantially higher classification, so that fewer than one in ten members of Congress had a staffer with sufficient clearance to review it. This was just another example, Mr. Gellman said, of why a classified designation alone should not dictate whether the media should publish.



## Counterterrorism Technology — the New York City Experience: Privacy and Constitutional Implications

**Moderator:** Professor Matthew Waxman, Columbia Law School

**Panelists:** David Raskin, Clifford Chance  
Douglass Maynard, New York City Police Department  
Andrew Weissmann, NYU School of Law Center for Law and Security and  
Center on the Administration of Criminal Law  
Faiza Patel, NYU School of Law Brennan Center for Liberty and  
National Security



This panel featured a discussion in the ongoing debate about balancing liberty and security, with a particular focus on the New York City experience. Professor Matthew Waxman began the discussion by noting that debates about privacy and security are often focused on the activities of the federal government, even though for most people the laws and policies of local government set the balance — especially in a place like New York City. With that observation, Professor Waxman invited Douglass Maynard, who at the time of this panel, served as the Deputy Director for Legal Affairs for the New York City Police Department (the “NYPD”), to discuss the new techniques and technologies that the police department is using.

Mr. Maynard first observed that there is a tendency to view the September 11 attacks as an “iconic and historic” event that is “significant but almost distant.” In fact, he said, there have been 16 terrorist plots against New York City since then. The ongoing threat is very real, and the threat is evolving, he said. Terrorists are using social media to exhort Westerners to take action. For example, there is an online terrorist magazine called *Inspire* that is very “slick” and that functions as a how-to manual for terrorists. The Tsarnaev brothers, charged with the Boston marathon bomb explosions, learned how to build their bombs from *Inspire*.

What can be done about these threats in New York City? Mr. Maynard said the NYPD does not have the resources of the NSA, and so it relies mostly on its officers to engage in quite traditional surveillance. The NYPD has the advantage of being a diverse police force that

reflects the diversity of the City, and gives the department a deep understanding of institutions and different cultures.

Mr. Maynard then highlighted one non-traditional investigative tool: the Domain Awareness System, which is a computer system that correlates information the NYPD has already gathered. The concept is similar to a detective looking at three case files at the same time, only Domain Awareness does it better and faster. The information processed includes 911 calls, video feeds, chemical alert systems and license plate readers.

Professor Waxman then turned to David Raskin, the former head of the terrorism unit in the U.S. Attorney's Office for the Southern District of New York, and asked him to address whether the way data is analyzed and aggregated in systems like Domain Awareness raises concerns distinct from the initial collection of that data.

Mr. Raskin said that since September 11, the government has installed thousands of street cameras that can zoom in and out and can follow people or objects. Information from these cameras is integrated with various other streams of information. Cameras, Mr. Raskin said, have undoubtedly been helpful in investigating terrorism after the fact. Closed circuit cameras identified the Tsarnaev brothers and were critical in identifying the 2005 London subway bombers.

Mr. Raskin noted that the Domain Awareness system is lauded for something different — the ability to use real-time surveillance to detect and prevent attacks. There is a legitimate privacy concern raised with real-time surveillance, especially with a system like Domain Awareness that has "largely no oversight." There is no judicial oversight, and the internal Police Department guidelines give extensive discretion.

Balanced against that concern is the more fundamental question of whether these systems have ever helped prevent a terrorist attack. Domain Awareness did not prevent Najibullah Zazi from bringing explosives into the New York subway system, and it did not detect Faisal Shahzad when he tried to bomb Times Square. That attempt was thwarted when a hot dog vendor alerted the police. The deterrent value is unclear, Mr. Raskin said, especially with terrorists on a suicide mission.

Professor Waxman then turned the discussion to Andrew Weissmann, who formerly served as the FBI's General Counsel. Mr. Weissmann discussed a set of internal FBI rules called the Domestic Investigations Operations Guide that attempts to address privacy concerns. By way of background, he explained, FBI investigations are divided into three categories: assessments, preliminary investigations and full investigations. At each stage, the FBI must have a stronger factual basis to suspect wrongdoing and, accordingly, is given access to more investigative tools.

Mr. Weissmann said the greatest concerns regarding privacy and big data arise in the assessment phase. To open an assessment, agents do not need any factual predicate; they need only have an authorized purpose. At the assessment stage, agents do not have the power of grand jury subpoenas, search warrants or wiretapping authority.

Mr. Weissmann offered as an example of an assessment the case of Tamerlan Tsarnaev, one of the Boston marathon bombers prior to the attack. The FBI opened an assessment and thus was permitted to conduct consensual interviews and review various law enforcement databases. Based on that limited investigation, there was no reason to suspect wrongdoing and the assessment was closed. This was necessary because the rules do not allow an open-ended assessment. By the time Mr. Tsarnaev traveled back to Russia and posted extremist material online, the FBI was no longer authorized to investigate him.

Another way the FBI rules address privacy is by restricting how data can be used after it is collected. This type of privacy protection generally falls outside the Fourth Amendment, which is focused on the initial collection. For every new investigative program, the FBI has several privacy lawyers focused on the question of how to limit the use of the data collected.

Professor Waxman then turned the discussion to Faiza Patel. Ms. Patel said she wanted to "take the lens out a little bit." Discussions of privacy and security tend to focus on terrorism, but, in fact, the tools for monitoring are used in all types of routine criminal cases. They are used in the context of public safety and in dealing with demonstrations like Occupy Wall Street.

It also is important to keep in mind, Ms. Patel said, that data aggregation and collection are almost always "about people who haven't done anything wrong and people who aren't even suspected of doing anything wrong." License plate readers, video cameras and location tracking gather data on everyone, not just criminals. Governments now have the capability to use a device called a Stingray, which basically mimics a cell phone tower, to read location data without having to go to the phone companies or get a court order.

Other areas of indiscriminate data collection include facial recognition technology, credit card data and public motor vehicle and school records. The "common thread" is "indiscriminate collection involving primarily non-criminal activity."

Ms. Patel said that these data gathering tools are touted as deterring crime, but that this claim is far from clear. She referred to a study of 13 police districts in London that installed video cameras. There was a statistically significant crime drop in only one district and an increase in crime in six.

The data gathering tools also are touted for being able to predict terrorist attacks, but Ms. Patel said that this claim is doubtful. The use of big data to predict consumer spending habits is based on millions of purchasing decisions, but terrorist attacks are very few, and each is distinctive. There is no evidence of big data predicting or preventing one.

Ms. Patel said that these threats to liberty pose a unique challenge because of the lack of democratic controls. Whereas a law enforcement policy like stop-and-frisk is highly visible in a community and can be the subject of a vigorous political response, it is harder for the public to respond to tactics when citizens are not informed about what the government is doing.

Professor Waxman invited Mr. Maynard to respond.

Mr. Maynard first noted that the Domain Awareness System was not intended to be a “magic machine” to identify terrorists and that it should not be judged by that standard. He added that the deterrent effect of systems like Domain Awareness cannot be overstated: “The attack that doesn’t happen is one you never know about.” He offered two examples to suggest the value of deterrence. First, a suspect named lyman Faris was scouting the Brooklyn Bridge for a potential attack, but reported to his co-conspirators that it was “too hot,” i.e., that there was too much surveillance. Second, the terrorist magazine *Inspire* praised the Tsarnaev brothers for having chosen Boston because it was “relatively out of the enemy’s attention,” unlike New York. For all the privacy concerns about video cameras, Mr. Maynard stated that the public and politicians actually want more cameras.

Mr. Maynard then said the NYPD policy protects privacy through various internal policies, including policies about data destruction. Videos, for example, are destroyed automatically after 30 days, and license plate information after five years. There is limited access within the department to surveillance data, and there is a complete audit trail of who accessed what data and when.

Mr. Maynard disagreed with Ms. Patel's suggestion that there was limited democratic accountability because, from his perspective, the NYPD's policies are subject to extensive political and media attention.

Professor Waxman then asked: Are these new technologies “game changing,” and, if so, how does law and policy address that?

Ms. Patel agreed that “we’re at a game changing moment” because it is so easy and cheap to aggregate data about people. The law is beginning to catch up. Ms. Patel referred to the Supreme Court’s decision in *United States v. Jones*, 132 S. Ct. 945 (2012), which recognized that the Fourth Amendment can be triggered with ongoing location tracking. She also mentioned the Eleventh Circuit’s decision from the prior week in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), which held that a warrant was necessary for cell phone location information.

Mr. Weissmann also agreed with the “game changer” characterization, but highlighted that advancing technology was being used by criminals and terrorists too. He added that the focus of discussion tends to be on technology enabling the government to collect too much, but what is often missing is the countervailing concern of technology preventing the government from collecting anything. Terrorists and criminals can use technology to communicate in ways the government cannot monitor — i.e., “going dark.” That is why it is imperative, he said, for there to be the capability to intercept communications, irrespective of the legal standard used to determine when it is permissible to do so. Mr. Weissmann said that the fix for the problem of “going dark” needs to come from Congress, but he doubted that Congress was likely to act.

## **Report of the 2012-2013 and 2013-2014 Supreme Court Terms**

**Speaker:** Associate Justice Ruth Bader Ginsburg



United States Supreme Court Justice Ruth Bader Ginsburg's report on the preceding year's Supreme Court term is an annual highlight of the Judicial Conference. Because the 2013 Judicial Conference was canceled, Justice Ginsburg's report covered the 2012-2013 term, as well as the recently-completed 2013-2014 term. Justice Ginsburg reported on the numbers of cases briefed and argued in both terms and provided statistics on the percentage of cases decided unanimously (49% in 2012-2013 and 46% as of the date of the Conference in 2013-2014) and by five to four or five to three votes (30% in 2012-2013 and 10% in 2013-2014, but, as Justice Ginsburg noted, "likely to increase" in the weeks following the Judicial Conference). She also provided information on the Justices most likely to agree (Justices Ginsburg and Kagan) and to disagree (Justices Ginsburg and Alito), the Justice most likely to be in the majority (Justice Kennedy for the fifth consecutive term in 2012-2013, who voted with the majority in 91% of cases during that term), and the Justice who was most active at oral argument (Justice Sotomayor, who asked an average of 21.6 questions per argument in the 2012-2013 term, narrowly outpacing Justice Scalia, who asked an average of 20.5 questions per argument during that term). She also provided information on rulings from the Second Circuit reviewed by the Court during the two terms: ten cases in 2012-2013, six of which were reversed and four of which were affirmed, and five cases in 2013-2014, two of which had been affirmed and one of which had been reversed as of the date of Justice Ginsburg's report.

Justice Ginsburg then reviewed significant cases decided by the Supreme Court during the two terms, with a particular focus on cases coming to the Supreme Court from the Second Circuit. Among other cases, Justice Ginsburg discussed *Town of Greece v. Galloway*, 134 S. Ct. 1811 (2014), *Schuette v. Coalition to Defend Affirmative Action*, 134 S. Ct. 1623 (2014), *McCutcheon v. Federal Election Commission*, 134 S. Ct. 1434 (2014), *United States v. Windsor*, 133 S. Ct. 2675 (2013), *Shelby County v. Holder*, 133 S. Ct. 2612 (2013), *Agency for International Development v. Alliance for Open Society International*, 133 S. Ct. 2321 (2013), *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013) and *Kirtsaeng v. John Wiley & Sons*, 133 S. Ct. 1351 (2013).

For Justice Ginsburg's remarks on these cases, as well as cases from the 2013-2014 term that had not yet been decided as of the date of the Conference, please see Appendix B, which contains the full text of Justice Ginsburg's report.



## Dialogue with Justice Ginsburg

**Participants:** Associate Justice Ruth Bader Ginsburg  
Honorable Mae D'Agostino  
Honorable Richard J. Arcara



Another annual highlight of the Judicial Conference is the opportunity to hear from Justice Ginsburg as she is interviewed by judges from the Circuit. This year, Conference-goers were treated to a special performance of vocal selections from a new opera by Derrick Wang called *Scalia/Ginsburg*, which was inspired by the opinions of Supreme Court Justices Antonin Scalia and Ruth Bader Ginsburg. Mr. Wang and vocal artists from Opera Saratoga performed selections from the opera, while United States District Judges Richard Arcara (WDNY) and Mae D'Agostino (NDNY) interviewed Justice Ginsburg about the opera, other aspects of her relationship with Justice Scalia and her approach to judicial decision-making.

A copy of the handout that accompanied the performance is attached as Appendix C.



## Cyber-Terrorism and the Private Sector: Responses and Liabilities

**Moderator:** Professor Karen J. Greenberg, Fordham Law School

**Panelists:** David F. Snively, Secretary and General Counsel, Monsanto Company  
Richard Salgado, Director of Law Enforcement, Google  
Honorable Louis J. Freeh, Freeh Group International Solutions, LLC  
John Thorne, Kellogg Huber Hansen Todd Evans & Figel PLLC



The Judicial Conference concluded with a panel that explored cyber-crime and cyber-terrorism from the perspective of the private sector. A panel featuring voices from academia, prior government service, and corporate leadership, provided an important complement to earlier panels that had explored governmental responses to, and perspectives on, the cyber-threat.

Professor Karen J. Greenberg, Director of the Center on National Security at Fordham Law School, moderated the panel. Professor Greenberg began the panel discussion by stating that the purpose of the panel was to discuss the “elephant in the room” from the prior days’ discussions: the role of the private sector in protecting our security and, more importantly, “what should be the role of the private sector in its relationship to government.” Professor Greenberg indicated that she intended the panel to address the “conversation” between the government and the private sector concerning civil liberties, regulation and the rights of corporations to make their profits. She asked John Thorne, former Deputy General Counsel of Verizon Communications, to commence the discussion by expressing his views concerning the responsibilities, liabilities and future of private sector regulation in the cyber-age.

Mr. Thorne commenced by relating how, when he was still working at Verizon, he was first asked to address cyber-security and privacy issues in the mid-2000s after Verizon acquired assets of telecommunications provider MCI and the company had to upgrade its infrastructure to integrate those assets. Mr. Thorne stated that Verizon determined that substantial investments in

security and privacy would benefit the company by helping it to enable a “more secure, more private, better experience for customers,” and help it increase market share. He stated that their efforts resulted in increased consumer confidence in the company, but that the process was an intensive one, somewhat like “undergoing an audit” to determine the company’s weaknesses and vulnerabilities. Mr. Thorne recommended that judges evaluating evidentiary issues involving cyber-matters consider creating what he described as an “audit privilege” to encourage companies to inspect themselves, identify opportunities for improvement and track reforms that they make without risking adverse legal consequences as a result of their awareness of vulnerabilities.

Mr. Thorne then turned to the current state of the law concerning communications firms, other private enterprises and critical infrastructure. He stated that the “good news for critical infrastructure companies is that almost everything at the moment is completely voluntary” due to the absence of statutes or binding codes of conduct governing how critical infrastructure firms need to act in the cyber-world. The “bad news,” however, was that the absence of regulation creates a “terrific opportunity for exposure when something goes wrong and the very flexible tort and contract doctrines are available for people who want to create a case if something bad happens to their information or something terrible happens that knocks out the things that rely on the critical infrastructure.” Mr. Thorne recommended adoption of a standard process developed by the National Institutes of Standards and Technology called the “Framework for Improving Critical Infrastructure Cybersecurity” (the “NIST Framework”) to help figure out vulnerabilities and to address and track the necessary improvements.<sup>4</sup> Mr. Thorne stated that a significant motivation in today’s world for adequately protecting information is that if the information is not protected properly, “you’re going to lose your job.” He noted a further motivation: inadequate data protection could result in adverse action by the Federal Trade Commission (“FTC”) and the Federal Communications Commission (“FCC”), among other federal regulators, citing examples of recent actions and statements by those regulators in which, among other things, a company’s inadequate control of customer data could constitute an “unfair and deceptive” act subject to sanction by the FTC. He noted, however, that the NIST Framework has to be adopted by top management of a company to be successful and to guard against potential liability.

Professor Greenberg then asked Richard Salgado, a former federal prosecutor and now a Google executive, how the revelations by Edward Snowden concerning the government’s covert efforts in the cyber-world affected the conversation between government and the private sector concerning cyber-matters. Mr. Salgado started by stating that, at Google “privacy and security are really kind of the same thing.” Google is interested in protecting the data of all users, no matter where in the world they are located, from “those who have no authorized access to their data.” Those without authorized access might include hackers from foreign nation-states or actors within the United States, including intelligence services. Mr. Salgado related that Google first experienced the issue in a significant way in 2009 when Chinese hackers intruded into the Google network. He stated that Google decided, “we were

---

<sup>4</sup> A copy of the NIST Framework is available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

not going to be shamed by it, we were going to investigate like crazy" to "figure out what happened, fix our systems, get secure so it doesn't happen again and catch it if there are any attempts." The information gained from the investigation then was reported to the government and to other companies that Google determined may have suffered from the same attack. After Google went public with the attack and its response to it, other companies started disclosing their own experiences with cyber-attacks, leading Mr. Salgado to conclude that Google's efforts may have broken "some sort of shame barrier" that had been keeping other companies from talking about cyber-security issues that they were experiencing from China and other jurisdictions. Over time, as Mr. Salgado reported, the culture of companies had changed to "working with each other to share vulnerability information and help each other out in the investigations."

Mr. Salgado related that, while information-sharing among companies has proven successful, it has "proven tricky once you introduce government into that." This concern arises because the law imposes restrictions on the types of information that can be shared with the government. There are risks that the government will take "aggressive action against the company" and result in businesses turning over more data to the government if issues are brought to the government's attention. In Mr. Salgado's view, the role of government in these conversations among companies was not fully worked out, and there are "a lot of improvements that need to be made."

Responding to Professor Greenberg's question, Mr. Salgado stated that the revelations concerning Edward Snowden had not affected Google's approach to security significantly because Google's approach to security was and continues to be "all about keeping data secure from those that aren't authorized to see it," including state actors. He indicated that stories relating to federal intelligence services' alleged secret efforts to weaken security in products to make it easier to breach encryption and to pick up communications between data centers were "of concern" and that Google's reaction was to "find where those vulnerabilities are and to secure them so there aren't ways to get the data that aren't part of the legal regime" through the criminal or national security legal processes. He stated that the Snowden revelations prompted Google to speed up encryption and other security efforts that already were underway before the revelations. Mr. Salgado also reported that the revelations have caused Google to review legal authorities in the United States and to work hard, "not only to be transparent with users about the demands" from government under the current legal regime, but to try to "update the laws to make them match what users should usually expect will happen to their data when the government comes knocking on Google's door."

Professor Greenberg then asked former FBI Director and United States District Judge Louis J. Freeh to offer his perspective on the role the government should play in cyber-security. Judge Freeh began by relating that issues concerning technology, security and privacy had been faced by the country since the days of Benjamin Franklin, who used to write and struggle with the balance between liberty and security. He stated that if those issues were hard in the 18<sup>th</sup> century, they are "exquisitely complex" now, too exceptional of a problem for the government to address by itself. He gave as an example the creation of the Economic Espionage Act in the 1990s, which enabled the government to prosecute cyber-thefts of intellectual property. He related that the State Department raised objections to the Act because it was concerned that

the word “espionage” would be offensive to most of those who were stealing our intellectual property, who were “our closest allies.” Judge Freeh related that the sophisticated and problematic political issues related to intellectual property made it difficult for the government to organize and deal with economic espionage. He indicated that, as a result, the government can play a role in protecting intellectual property, but it “can’t play a controlling role” in that effort. He cited as a further example the fact that in the 24 months it takes to develop and adopt a government regulation, computing power doubles, and that technological change often outpaces the ability of government to regulate it.

Professor Greenberg then turned to David F. Snively, and asked him for practical examples, based on his experiences at Monsanto, of how a company guards against and responds to cyber-attacks. Mr. Snively explained that cyber-security now sits “at the top of any board of directors’ list of concerns.” He explained that, for Monsanto, a science company that focuses on agriculture, intellectual property is its “crown jewels.” He stated that to protect those “crown jewels,” the company has developed substantial resources for monitoring its Information Technology (“IT”) and security systems around the globe. It has mapped all of its information to determine where it is housed, so that if there is a loss or a breach, “we can at least understand where our vulnerabilities are.” He revealed that, despite this effort, Monsanto is “attacked on average 490,000 times a month.” Due to the sheer volume of attacks, and the presence of subsidiaries and employees around the world who have personal devices or computers, there have been occasions in which attacks have breached Monsanto’s security.

Mr. Snively gave as an example a recent occasion on which state-sponsored hackers attempted to access Monsanto’s headquarters and its Silicon Valley presence, but they did not succeed. Those same hackers, however, were able to breach the cyber-security systems of a recently-acquired subsidiary and access the subsidiary’s data systems for a brief period of time before the breach was detected. He described the intrusion as being contained quickly and addressed in a relatively straightforward manner. However, because the intrusion had accessed the “top levels of the servers in that subsidiary,” and it was not possible to determine whether the intruders had accessed data hosted on that subsidiary’s servers, including private information concerning employees and customers of the subsidiary, it became necessary under state privacy laws to carry out procedures to notify those employees and customers of the breach, which then prompted media reports on the breach and potential adverse business consequences as the breach was publicized. The company also determined that it would cover costs of all of the employees’ and customers’ issues arising out of the breach, including credit searches. Disclosures to state attorneys general and governments located abroad were necessary. He described the undertaking as an expensive one, even where, as in that case, the breach was detected quickly and it was impossible to determine if anything of value was taken. Mr. Snively stated that the high costs were not uncommon — that data breaches, on average, cost Monsanto \$3 million per breach to address.

Mr. Snively explained further that Monsanto has developed a threat matrix concerning the cyber-threat with three bundles: advanced, persistent threats, which include state-sponsored attacks and sophisticated hackers like LulzSec and Anonymous; generalized activist groups who engage in cyber-attacks; and internal threats in which an employee, accidentally

or on purpose, breaches the company's cyber-security. He described the internal threat as the most serious one because internal actors are "the people you trust," who are "going to get all the way to the edge of your crown jewel data" and cause substantial issues if the data is lost or stolen.

Professor Greenberg then asked Mr. Snively whether information on data breaches and responses was shared within his industry, and whether this cut against the argument that the private sector cannot respond effectively to the cyber-threat because of its interests in avoiding public disclosures that risk reputational harm. Mr. Snively replied that, generally, information was not shared within the industry for competitive reasons, but that Monsanto did share information about cyber-threats with other companies in the IT industry, and it had a policy of communicating breaches of cyber-security properly. He described the company's approach to the cyber-threat "almost as a standing crisis management approach," in which the company was prepared to respond quickly and effectively to cyber-threats and access resources either inside or outside its sector.

Judge Freeh added that disclosure issues were complicated by corporate fiduciary duties and regulatory issues. He explained that, with respect to publicly traded companies, material breaches of cyber-security might have to be reported to an auditor, which could then lead to a debate concerning whether a breach was material enough to warrant a public disclosure. A decision to disclose then could prompt law enforcement agents to ask that the information not be disclosed publicly because of an ongoing investigation, which would raise very difficult issues for companies as they attempted to balance competing interests. Judge Freeh added that, "as these breaches get more material and more serious and the calculation of a loss much more difficult, you have to make a call and it's a very, very significant mistake to make if you make one."

Mr. Snively responded to Judge Freeh's comment by stating that Monsanto's response to cyber-breaches, as decided by the company's board of directors, was to disclose if there is any material breach, even if it adversely affects a government investigation, because of the risks to the company of non-disclosure.

Professor Greenberg then asked the panelists whether they foresaw legislation that would mandate particular approaches to the cyber-threat, and how companies would react if that happened. Mr. Thorne replied that, while there were many proposals for legislation, it would be hard to craft legislation that would be adopted. Mr. Thorne responded to comments earlier in the Conference by former U.S. Senator Joseph Lieberman in which he stated that in the absence of legislation, there would be massive exposure for private companies, by stating that he believed courts and regulatory agencies addressing breaches of cyber-security had the ability to fashion rules that limited companies' liability in an appropriate way.

Professor Greenberg then asked Mr. Salgado to address whether a conflict had developed between the IT industry and the government over the proper approach to the cyber-threat. She alluded to recent assertions by Microsoft that it would not cooperate with the government in providing certain information going forward and earlier similar statements by Yahoo! that appeared to reflect that "there has been a defiant sense on the part of industry."

Professor Greenberg asked why the conflict had developed, and what the IT industry was trying to protect through the conflict: "Is it your profits? Is it your sense of self, your identity?"

Mr. Salgado replied that he did not think that there was a war going on between the IT industry and government. He explained that Google and other Silicon Valley companies have a "very libertarian culture" in which there was a "great deal of suspicion around government intrusion into the privacy of the users' data." He also observed that the laws concerning privacy had not been keeping up with "what's really happening in the world," which was that information that used to be stored in homes is now getting out to the Internet, where it is stored and relied upon by users. He explained that the governing statute, the Electronic Communications Privacy Act, dated from 1986, is "a long time in Internet time." In Mr. Salgado's view, the third-party doctrine of *Smith v. Maryland*, under which information held by third parties is not entitled to Fourth Amendment protections, is not compatible with today's world, because "to live in today's modern world and participate in the modern economy you're going to have a hard time staying away from" companies that hold private information. Mr. Salgado indicated that he saw momentum towards changing the laws to increase privacy, but that this was not a war as much as a desire in the IT industry to change the rules to increase privacy protections for users. He indicated that this conflict over existing law is, in some cases, playing out in the courts as companies begin challenging government data-collection efforts and programs, such as novel requests under the Foreign Intelligence Surveillance Act or requests for bulk data collection under the Patriot Act.

Professor Greenberg then asked Judge Freeh how he saw the role of government, the courts and private companies developing over time. Judge Freeh replied that he did not believe "volunteerism" by companies to address cyber-threats would be sufficient, given that voters and consumers do not believe that private companies are meeting their expectations concerning cyber-security. He cited as an example the SEC's recent move to require financial institutions to disclose cyber-security plans, vulnerability assessments and other matters in response to SEC inspections and examinations. Judge Freeh also observed that courts in the First and Fourth Circuits are considering whether to impose tort liability on service providers if there are data breaches so that losses do not fall only on consumers. The disconnect between corporations' efforts, while diligent, and expectations and political demands, has led Judge Freeh to conclude that legislation in the field is inevitable.

Professor Greenberg then asked the panelists to discuss whether the growing cyber-threat is coming more from corporate criminals versus state actors. Mr. Thorne replied that he lacked statistics on the sources of the threats, but he noted that what is known as the "Internet of things" — the connection to the Internet of more and more devices — was growing exponentially, so that by 2020 "we will have added 50 billion more things to the Internet." Mr. Thorne indicated that increased connectivity would result in more vectors for different actors to attack, making it critical for both government and private actors to do more to guard against threats.

Mr. Salgado replied that, while he could not divide up the source of attacks between private and state actors, Google is under "constant attack." He gave as an example Distributed

Denial of Service ("DDOS") attacks, which he asserted were constantly being attempted against Google, sometimes in significant ways. Mr. Salgado replied that Google had developed a high ability to absorb and fend off DDOS attacks, but it was not possible to know the motive for the attacks — whether attackers are just "angry at somebody's blog post or trying to make some bigger point."

Mr. Salgado added that, following the 2009 attack from China, Google developed a robust network security program that enables Google to determine whether phishing emails are being sent from particular actors to particular types of users, such as state actors who may target government employees' Gmail accounts for intrusion. He stated that when these attacks are detected, Google not only blocks the emails, it also informs users that it believes they have been targeted by state-sponsored attackers and advises them to take steps to secure their accounts.

Professor Greenberg asked Mr. Salgado whether Google informs the government when it detects such attacks. He replied that while the user can inform the government, Google does not. Mr. Salgado stated that, while Google has teams that investigate crimes and reports them to the government, it is very cautious about turning over user information to the government, particularly where the user is a victim. Its policy is to let users decide whether they want to be involved in a criminal investigation. It is only where a "bad guy" is detected that a referral may be made, and even in that case, legal process is necessary for there to be further disclosures so that it is all "very tight and user privacy oriented."

Judge Freeh added that there were two types of significant threats to cyber-security: internal threats and external threats. He described the internal threat as "huge, unmeasured and really uncontrolled." With respect to external threats, Judge Freeh described the state actors as "clearly the heavy lifters" in the arena. He explained that some state actors had "the potential and the wherewithal to literally shut down other countries and their systems and their infrastructure." He explained that it is not done, just as our nation does not shut down banking channels used by terrorists, even though we could, because of the negative repercussions that would flow from shutting down third-party banking systems. He analogized it to experience during cold war where "everyone had these massively destructive weapons, [but] no one actually used them." He added that some state actors even in radical regimes had the ability to inflict significant damage but did not do so due to practical, economic and personal constraints. The increased capabilities of non-state actors, however, changed the dynamic because they "don't have the hesitations and controls that a state actor might have."

Professor Greenberg asked Mr. Snively whether he had "better news than that." He replied that he did not. He explained that the cyber-threat was real and not going to stop and that Monsanto constantly was under threat by state actors and others who would attempt to steal its intellectual property. He added that judges also needed to pay attention to the cyber-threat in order to ensure the integrity of the legal system "because there's a lot of money that's going to change hands in this arena and this is something you're going to live with every day."

Professor Greenberg concluded the panel by citing the need for public education "so that the kinds of threats that need to be taken seriously can be taken seriously and can be addressed as an issue."



## Appendix A: Speakers' Biographies



**Richard Arcara** was appointed by President Ronald Reagan as a United States District Judge for the Western District of New York and entered on duty on June 1, 1988. Judge Arcara served as Chief Judge from January 1, 2003 to December 31, 2009. He is a graduate of the Villanova University School of Law and St. Bonaventure University. Judge Arcara served in the United States Army from 1966 to 1967, first as a captain in the Military Police Corps in Korea and then as Provost Marshal at Edgewood Arsenal, Maryland.

Judge Arcara served two four-year terms as the District Attorney of Erie County, New York, winning election in 1981 and again in 1985. From 1975 to 1981, he served as the United States Attorney for the Western District of New York, serving under Presidents Ford, Carter and Reagan. In 1969, Judge Arcara was appointed as an assistant United States attorney, becoming First Assistant in that office in 1973. Prior to his government service, he was an associate attorney in private practice. During his tenure as Erie County District Attorney, Judge Arcara served as President of the New York State District Attorneys Association and as President of the National District Attorneys Association.

He is a member of the American Judicature Society and the National Association of Former United States Attorneys. Judge Arcara is the Second Circuit representative to the Committee on Court Administration and Case Management of the Judicial Conference of the United States. He previously served as a member of the JCUS Committee on Criminal Law. Judge Arcara is married to the former Gwendolyn Oliver.



**Preet Bharara** was appointed by President Barack Obama as the U.S. Attorney for the Southern District of New York and entered on duty on August 13, 2009. Prior to becoming the U.S. Attorney, Mr. Bharara served as Chief Counsel and Staff Director of the U.S. Senate Judiciary Committee's Subcommittee on Administrative Oversight and the Courts. From 2000 to 2005, Mr. Bharara served as an Assistant U.S. Attorney in the Southern District of New York, where he prosecuted a wide range of cases involving organized crime, racketeering, securities fraud, money laundering, narcotics trafficking, and other crimes. Mr. Bharara was a litigation associate in New York at Swidler Berlin Shreff Friedman from 1996 to 2000 and Gibson, Dunn & Crutcher from 1993 to 1996.

He graduated magna cum laude from Harvard College with an A.B. in Government in 1990, and from Columbia Law School with a J.D. in 1993, where he was a member of the Columbia Law Review.

As U.S. Attorney, Mr. Bharara oversees the investigation and litigation of all criminal and civil cases brought on behalf of the United States in the Southern District of New York, which

encompasses New York, Bronx, Westchester, Dutchess, Orange, Putnam, Rockland, and Sullivan counties. He supervises an office of more than 200 Assistant U.S. Attorneys, who handle a high volume of cases that involve domestic and international terrorism, narcotics and arms trafficking, financial and healthcare fraud, public corruption, gang violence, organized crime, and civil rights violations.

During Mr. Bharara's tenure as U.S. attorney, the office has successfully extradited and prosecuted one of the most notorious arms traffickers in the world, Viktor Bout; obtained a life sentence for the Times Square bomber; and convicted one of the Al Qaeda members responsible for plotting the 1998 bombings of two American embassies in East Africa.

In June 2012, the New York Times published an op-ed written by Mr. Bharara entitled, "Asleep at the Laptop," about the growing cyber threat to private industry.



**Michael Bosworth** currently serves as Special Counsel to James B. Comey, Jr., the Director of the Federal Bureau of Investigation. In that capacity, he advises the Director on a range of matters including national security and cyber crime. Previously, Mr. Bosworth worked in the U.S. Attorney's Office for the Southern District of New York, where he served as Co-Chief of the Complex Frauds Unit and Deputy Chief of the Public Corruption Unit. He successfully prosecuted former New York City Policy Commissioner Bernard Kerik, New York State Senator Carl Kruger, and financial adviser Kenneth Starr, and he supervised a range of cyber crime, intellectual property theft, tax fraud, FCPA, and other white collar prosecutions. Mr. Bosworth is a recipient of the National Association of Former U.S. Attorneys' J. Michael Bradford Award for being the most outstanding AUSA in the country, as well as the Federal Law Enforcement Foundation's Prosecutor of the Year Award. He clerked for the Hon. Stephen G. Breyer of the U.S. Supreme Court, the Hon. Robert A. Katzmann of the U.S. Court of Appeals for the Second Circuit, and the Hon. Jed S. Rakoff of the U.S. District Court for the Southern District of New York. Mr. Bosworth is a summa cum laude graduate of Princeton University and a graduate of Yale Law School, where he served as Comments Editor on the Yale Law Journal.



**Gary Brown** is Deputy Legal Advisor for the International Committee of the Red Cross, Regional Delegation for the United States and Canada, a position he has held since 2012. He provides advice on international humanitarian law and contributes to the strategic positioning of the ICRC and the Delegation on issues of international law. Prior to joining the ICRC, Mr. Brown served 24 years as a judge advocate with the United States Air Force. Colonel Brown's Air Force career included two tours in the United Kingdom and one in Panama, as well as two deployments to the Middle East. He spent a year at the Combined Air Operations Center, Southwest Asia as the senior lawyer advising on combat air operations in Afghanistan and Iraq. In his final assignment he was the first senior legal counsel for U.S. Cyber Command, Fort Meade, Maryland, where he served for three years.

Mr. Brown is a noted speaker on cyber operations law, and has authored several articles related to cyber warfare, including "Easier Said Than Done: Legal Reviews of Cyber Weapons," *Journal of Nat'l Security Law & Policy* (2014) (coauthor), "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Forces Quarterly* (2011), "Law at Cyberspeed," *Int'l Humanitarian Law & New Weapon Technologies* (2012), "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* (2012) (coauthor) and "On the Spectrum of Cyberspace Operations," *Small Wars Journal* (2012) (coauthor). He was the official U.S. observer to the international group of experts drafting the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). He is a graduate of the University of Nebraska College of Law, and holds an LL.M. in international law from Cambridge University.



**Daniel Cahen** serves as the Legal Advisor for the Washington Regional Delegation for the United States and Canada. In this capacity, he is responsible for legal support to the ICRC in the U.S. and Canada, with a particular focus on Guantanamo and detention policy issues, as well as military operations notably in Afghanistan and Iraq. Before assuming his present functions, Mr. Cahen was Deputy Head of the Legal Advisors to the Operations Units at the Headquarters of the ICRC in Geneva, where he advised ICRC teams based in Latin America, the Horn of Africa and South Asia on matters related to International Humanitarian Law. Before joining the Legal Division of the ICRC in Geneva in 2005, Mr. Cahen carried out assignments in ICRC field offices in Afghanistan, the Democratic Republic of Congo and Colombia.

He also worked as an attorney and was a member of the Paris Bar in France. He holds an LLB (King's College London), a Master's Degree in International Humanitarian Law and International Human Rights Law (University Paris II Panthéon Assas) and a Master's Degree in Comparative Criminal Law (University Paris I Panthéon Sorbonne).



**Michael Chertoff** concentrates in the area of White Collar Defense and Investigations. In recent years, he has handled a series of federal investigations, including complex criminal and civil regulatory matters. He has advised major clients on SEC and Justice Department investigations and successfully served as the independent monitor of a major national healthcare company under criminal and civil investigation.

In addition to his legal work, Mr. Chertoff is Founder and Chairman of The Chertoff Group, a security and risk management firm, where he provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery.

In April of 2012, Mr. Chertoff was elected as the new Chairman of the Board of Directors of BAE Systems, Inc. He also sits on the board of directors or board of advisors of a number of companies and nonprofits.

Previously, Mr. Chertoff served as Secretary of the Department of Homeland Security where he led a 218,000 person department with a budget of \$50 billion. As DHS Secretary, Mr. Chertoff developed and implemented border security and immigration policy; promulgated homeland security regulations; and spearheaded a national cyber security strategy. From 2003 to 2005, Mr. Chertoff served on the U.S. Court of Appeals for the Third Circuit. Before becoming a federal judge, Mr. Chertoff was the Assistant Attorney General for the Criminal Division of the U.S. Department of Justice where he oversaw the investigation of the 9/11 terrorist attacks, and formed the Enron Task Force, which produced more than 20 convictions, including those of CEOs Jeffrey Skilling and Kenneth Lay.

Mr. Chertoff's career includes more than a decade as a federal prosecutor, including service as U.S. Attorney for the District of New Jersey, First Assistant U.S. Attorney for the District of New Jersey, and Assistant U.S. Attorney for the Southern District of New York. As a federal prosecutor, Mr. Chertoff investigated and personally prosecuted significant cases of political corruption, organized crime, and corporate fraud.

From 1994-2001, Mr. Chertoff represented major corporations and individuals in numerous white collar investigations and trials. Among other matters, he successfully represented the nation's largest hospital company in a four year, multi-jurisdictional criminal and civil investigation, represented major corporations in corruption scandals, and obtained acquittals at trial for individual criminal defendants.

Mr. Chertoff has received numerous awards including the Department of Justice Henry E. Petersen Memorial Award (2006), the Department of Justice John Marshall Award for Trial of Litigation (1987), NAACP Benjamin L. Hooks Award for Distinguished Service (2007), European Institute Transatlantic Leadership Award (2008), and two honorary doctorates. His trial experiences have been featured in over half a dozen books and many news articles.



**Sarah Cleveland** is a noted expert in international law and the constitutional law of U.S. foreign relations, with particular interests in the status of international law in U.S. domestic law, international humanitarian law, human rights law, and the constitutional law of U.S. foreign relations. From 2009 to 2011, she served as the Counselor on International Law to the Legal Adviser at the U.S. Department of State, where she supervised the office's legal work relating to the law of war, counterterrorism, and Afghanistan and Pakistan, and assisted with its international human rights and international justice work. She is the U.S. Observer Member to the Venice Commission of the Council of Europe, a member of the Secretary of State's Advisory Committee on International Law, and a member of the American Law Institute. Cleveland has testified before Congress on U.S. terrorism detention policy, the relevance of international law in constitutional interpretation, and the interdiction of Haitian refugees, and has provided evidence to the U.K. Parliament. She is currently co-director of the Project on Harmonization of the Law of Armed Conflict, and has been involved in human rights litigation in the United States and before the Inter-American Court of Human Rights. A former Rhodes Scholar, Ms. Cleveland holds a baccalaureate degree from Brown University, a master's degree from Oxford University and a J.D. from Yale Law School. She

clerked for Supreme Court Justice Harry Blackmun and Judge Louis Oberdorfer on the United States District Court for the District of Columbia. Before joining the Columbia Law School faculty in 2007, she previously taught at the Harvard, Michigan, and University of Texas law schools and at Oxford University.



**Mae Avila D'Agostino** is a United States District Judge for the Northern District of New York. At the time of her appointment in 2011, she was a trial attorney with the law firm of D'Agostino, Krackeler, Maguire & Cardona, PC. Judge D'Agostino is a 1977 magna cum laude graduate of Siena College in Loudonville, New York. At Siena College, Judge D'Agostino was a member of the women's basketball team. After graduating from college, she attended Syracuse University College of Law, receiving her Juris Doctor degree in May 1980. At Syracuse University College of Law, she was awarded the International Academy of Trial Lawyers award for distinguished achievement in the art and science of advocacy.

After graduating from Law School, Judge D'Agostino began her career as a trial attorney. She has tried numerous civil cases including medical malpractice, products liability, negligence, and civil assault.

Judge D'Agostino is a past chair of the Trial Lawyers Section of the New York State Bar Association and is a member of the International Academy of Trial Lawyers and the American College of Trial Lawyers. Judge D'Agostino has participated in numerous Continuing Legal Education programs. She is an Adjunct Professor at Albany Law School where she teaches Medical Malpractice. She is a past member of the Siena College Board of Trustees, and Albany Law School Board of Trustees. She is a member of the New York State Bar Association and Albany County Bar Association.



**Ashley Deeks** joined Columbia Law School in 2012 as an associate professor of law after two years as an academic fellow at the Law School. Her primary research and teaching interests are in the areas of international law, national security and the laws of war. She has written a number of articles on the use of force, administrative detention, the laws of war and the Iraqi constitution. Before joining the Columbia faculty in 2010, she served as the assistant legal adviser for political-military affairs in the U.S. Department of State's Office of the Legal Adviser, where she worked on issues related to the law of armed conflict, the use of force, conventional weapons, and the legal framework for the conflict with al-Qaida. She also provided advice on intelligence issues. In previous positions at the State Department, Ms. Deeks advised on international law enforcement, extradition and diplomatic property questions. In 2005, she served as the embassy legal adviser at the U.S. embassy in Baghdad, during Iraq's constitutional negotiations. Deeks was a 2007-08 Council on Foreign Relations international affairs fellow and a visiting fellow in residence at the Center for Strategic and International Studies.

Ms. Deeks received her J.D. with honors from the University of Chicago Law School, where she was elected to the Order of the Coif and served as comment editor on the Law Review. After graduation, she clerked for Judge Edward R. Becker of the U.S. Court of Appeals for the Third Circuit.



**Louis J. Freeh** is a partner and chair of the Executive Committee of Pepper Hamilton LLP. In 2007, Mr. Freeh founded Freeh Sporkin & Sullivan, LLP, a Washington, D.C. law firm, and the consulting firm Freeh Group International Solutions, LLC, of which he is chairman.

He graduated Phi Beta Kappa from Rutgers College in 1971, Rutgers School of Law in 1974 and New York University School of Law in 1984 (L.L.M.). In 1975, Mr. Freeh joined the Federal Bureau of Investigation (FBI) as a Special Agent, and was assigned to the New York City Field Division, and later at FBI Headquarters in Washington, D.C. Mr. Freeh served as a First Lieutenant in the United States Army Judge Advocate General Corps.

In 1981, Mr. Freeh joined the United States Attorney's Office for the Southern District of New York as an Assistant United States Attorney, later serving as Associate and Deputy United States Attorney. In 1991, Mr. Freeh was appointed by President George H.W. Bush as a United States District Court Judge for the Southern District of New York.

In 1993, President William J. Clinton appointed Judge Freeh as the Fifth Director of the Federal Bureau of Investigation. In 2001, Mr. Freeh joined MBNA America Bank in Delaware as vice chairman and general counsel.

Mr. Freeh is an advisor to Millennium Partners, L.P. and also a board member of the U.S. Naval Academy Foundation and the Max Planck Florida Institute. From 2006 to 2013, Mr. Freeh was a member of the Bristol-Myers Squibb Company Board of Directors, where he chaired the Governance Committee. Mr. Freeh and his wife, Marilyn, have six sons.



**Barton Gellman**, a critically honored journalist and author, is senior fellow at the Century Foundation and Lecturer at Princeton's Woodrow Wilson School. He is researching a book on the NSA, Silicon Valley and the surveillance-industrial revolution.

Mr. Gellman is one of three journalists who received archives of classified NSA documents from Edward Snowden in the spring of 2013. He broke the PRISM story in the first week of June and has since anchored The Washington Post's coverage of surveillance, privacy and security. In December, he was the first journalist to visit Snowden in Moscow, conducting 14 hours of interviews over two days.

His previous books include the bestselling *Angler: The Cheney Vice Presidency* (New York Times Best Books of 2008) and *Contending with Kennan: Toward a Philosophy of American Power*.

Mr. Gellman left the Washington Post in 2010, where he served tours as legal, military, diplomatic, and Middle East correspondent, to pursue book and magazine projects. He returned temporarily for the Snowden story. He graduated with highest honors from Princeton and earned a master's degree in politics at University College, Oxford, as a Rhodes Scholar.

His professional honors include two Pulitzer Prizes, the Los Angeles Times Book Prize, the George Polk Award, the Henry Luce Award, Harvard's Goldsmith Prize for investigative reporting and the Sigma Delta Chi medallion from the Society of Professional Journalists.

Online he can be found at bartongellman.com, @bartongellman and on his Century Foundation fellow's page.



**Ruth Bader Ginsburg** was nominated by President Clinton as Associate Justice of the United States Supreme Court in June 1993 and took the oath of office on August 10, 1993. Prior to her appointment to the Supreme Court, she served from 1980 to 1993 on the bench of the United States Court of Appeals for the District of Columbia Circuit. From 1972 to 1980, Justice Ginsburg was a professor at Columbia University School of Law. From 1963 to 1972, she served on the law faculty of Rutgers, the State University of New Jersey. She has served on the faculties of the Salzburg Seminar in American Studies and the Aspen Institute for Humanistic Studies, and as a visiting professor at many universities in the United States and abroad. In 1978, she was a Fellow at the Center for Advanced Study in the Behavioral Sciences in Stanford, California.

Justice Ginsburg has a B.A. degree from Cornell University, attended Harvard Law School, and received her LL.B. (J.D.) from Columbia Law School. She holds honorary degrees from Lund University (Sweden), American University, Vermont Law School, Georgetown University, DePaul University, Brooklyn Law School, Hebrew Union College, Rutgers University, Amherst College, Lewis and Clark College, Radcliffe College, New York University, Columbia University, Smith College, Long Island University, University of Illinois, Brandeis University, Wheaton College, Jewish Theological Seminary of America, George Washington University Law School, Northwestern University, the University of Michigan, Brown University, Yale University, Johns Hopkins University, John Jay College of Criminal Justice, University of Pennsylvania, Willamette University, and Princeton University.

In 1972, then-Professor Ginsburg was instrumental in launching the Women's Rights Project of the American Civil Liberties Union. Throughout the 1970s she litigated a series of cases solidifying a constitutional principle against gender-based discrimination. Her bar association activities have included service on the Board of Editors of the American Bar Association Journal, and as Secretary, Board member, and Executive Committee member of the American Bar Foundation. Justice Ginsburg served on the Council of the American Law Institute, and is a member of the Council on Foreign Relations, the American Academy of Arts and Sciences, and the American Philosophical Society. She has written widely in the areas of civil procedure, conflict of laws, constitutional law, and comparative law.

Justice Ginsburg's late husband, Martin D. Ginsburg, was a professor of tax law at Georgetown University Law Center; her daughter, Jane C. Ginsburg, is a professor of literary and artistic property law at Columbia Law School; and her son, James S. Ginsburg, is a producer of classical recordings.



**Karen J. Greenberg** is the Director of the Center on National Security and Visiting Faculty at Fordham Law School, and a noted expert on national security, terrorism, and civil liberties. She is the author of *The Least Worst Place: Guantanamo's First 100 Days* (2009), which was selected as one of the best books of 2009 by The Washington Post and Slate.com. Ms. Greenberg is co-editor with Joshua L. Dratel of *The Torture Papers: The Road to Abu Ghraib* and *The Enemy Combatant Papers: American Justice, the Courts, and the War on Terror*; editor of the books *The Torture Debate in America* and *Al Qaeda Now*; and editor of the Terrorist Trial Report Card, 2001–2011. Her work has frequently been featured in The New York Times, The Washington Post, The Los Angeles Times, The San Francisco Chronicle, NPR, and on major news channels. Greenberg earned a Ph.D. from Yale University and a B.A. from Cornell University. She is a permanent member of the Council on Foreign Relations.



**Rich Gross** is the current Legal Counsel to the Chairman of the Joint Chiefs of Staff. A native of Knoxville, Tennessee, Brigadier General Gross attended the U.S. Military Academy at West Point, graduating in 1985 with a Bachelor of Science degree in Computer Science. He was commissioned in the U.S. Army as a second lieutenant in the Infantry. In 1993, he graduated from the University of Virginia School of Law with a Juris Doctor degree and entered the U.S. Army Judge Advocate General's Corps. In 2009, he graduated from the U.S. Army War College at Carlisle Barracks, PA, with a Masters in Strategic Studies.

As a judge advocate, Brigadier General Gross has served in a variety of legal assignments, to include serving as the chief legal advisor (Staff Judge Advocate) for the Joint Special Operations Command (JSOC), the International Security Assistance Force (ISAF) and U.S. Forces-Afghanistan (USFOR-A) and, prior to his current position, at U.S. Central Command. Brigadier General Gross has multiple combat deployments to both Iraq and Afghanistan with joint and special operations units. His decorations include the Defense Superior Service Medal with Oak Leaf Cluster, the Legion of Merit, the Bronze Star with two Oak Leaf Clusters, the Defense Meritorious Service Medal, the Army Meritorious Service Medal with Oak Leaf Cluster, and the Non-Article 5 NATO Medal. He is a recipient of the U.S. Army Ranger Tab, Master Parachutist Badge, Air Assault Badge, and Expert Infantryman Badge.



**William J. Hochul, Jr.** is the United States Attorney for the Western District of New York. As U.S. Attorney, Mr. Hochul is responsible for overseeing the prosecution of any federal criminal case brought within the seventeen counties of Western New York and also represents the United States in all civil matters brought within this territory.

Mr. Hochul graduated cum laude from the University of Notre Dame in 1981, and earned his law degree from the State University of New York at Buffalo Law School in 1984, where he won the Best Oralist award at the National Constitutional Law Moot Court competition held in North Carolina. After graduation, Mr. Hochul served as a law clerk to a Maryland Court of Appeals Judge. At the conclusion of this appointment, Mr. Hochul joined the litigation section at the Washington Office of a large international law firm, where he represented a wide variety of clients in complex civil litigation matters, including racketeering and fraud-related lawsuits.

In 1987, Mr. Hochul joined the Department of Justice as an Assistant United States Attorney for the District of Columbia. While in Washington, Mr. Hochul prosecuted an extensive array of violent and white collar criminal cases, and later specialized in the prosecution of first-degree and gang-related murder cases.

Mr. Hochul joined the United States Attorney's Office for the Western District of New York in 1991 where he prosecuted a large number of cases: notorious violent and white collar criminals, racketeering and other complex schemes, and multiple cases targeting violent street gangs and emerging international organized crime groups. Mr. Hochul became Chief of the Office's Anti-Terrorism Unit following September 11, 2001, and Chief of the National Security Division in 2006. While in these positions, Mr. Hochul served as lead prosecutor in several high-profile international terrorism cases, including the highly successful prosecution of the internationally known Lackawanna Six.



**Jeh Charles Johnson** was sworn in on December 23, 2013 as the fourth Secretary of Homeland Security. Prior to joining DHS, Secretary Johnson served as General Counsel for the Department of Defense, where he was part of the senior management team and led the more than 10,000 military and civilian lawyers across the Department. As General Counsel of the Defense Department, Secretary Johnson oversaw the development of the legal aspects of many of our nation's counterterrorism policies, spearheaded reforms to the military commissions system at Guantanamo Bay in 2009, and co-authored the 250-page report that paved the way for the repeal of "Don't Ask, Don't Tell" in 2010.

Secretary Johnson's career has included extensive service in national security and law enforcement, and as an attorney in private corporate law practice. Secretary Johnson was General Counsel of the Department of the Air Force from 1998 to 2001, and he served as an Assistant U.S. Attorney for the Southern District of New York from 1989 to 1991.

In private law practice, Secretary Johnson was a partner with the New York City-based law firm of Paul, Weiss, Rifkind, Wharton & Garrison LLP. In 2004, Secretary Johnson was elected a Fellow in the prestigious American College of Trial Lawyers, and he is a member of the Council on Foreign Relations.

Secretary Johnson graduated from Morehouse College in 1979 and received his law degree from Columbia Law School in 1982.



**Harold Hongju Koh** is Sterling Professor of International Law at Yale Law School. He returned to Yale Law School in January 2013 after serving for nearly four years as the 22nd Legal Adviser of the U.S. Department of State.

Professor Koh is one of the country's leading experts in public and private international law, national security law, and human rights. He first began teaching at Yale Law School in 1985 and served as its fifteenth Dean from 2004 until 2009. From 2009 to 2013, he took leave as the Martin R. Flug '55 Professor of International Law to join the State Department as Legal Adviser, service for which he received the Secretary of State's Distinguished Service Award. From 1993 to 2009, he was the Gerard C. & Bernice Latrobe Smith Professor of International Law at Yale Law School, and from 1998 to 2001, he served as U.S. Assistant Secretary of State for Democracy, Human Rights, and Labor.

Professor Koh has received thirteen honorary degrees and more than thirty awards for his human rights work, including awards from Columbia Law School and the American Bar Association for his lifetime achievements in international law. He has authored or co-authored eight books, published more than 180 articles, testified regularly before Congress, and litigated numerous cases involving international law issues in both U.S. and international tribunals. He is a Fellow of the American Philosophical Society and the American Academy of Arts and Sciences, an Honorary Fellow of Magdalen College, Oxford, and a member of the Council of the American Law Institute.

He holds a B.A. degree from Harvard College and B.A. and M.A. degrees from Oxford University, where he was a Marshall Scholar. He earned his J.D. from Harvard Law School, where he was Developments Editor of the Harvard Law Review. Before coming to Yale, he served as a law clerk for Justice Harry A. Blackmun of the United States Supreme Court and Judge Malcolm Richard Wilkey of the U.S. Court of Appeals for the D.C. Circuit, worked as an attorney in private practice in Washington, and served as an Attorney-Adviser for the Office of Legal Counsel, U.S. Department of Justice.



**Joseph I. Lieberman**, Senior Counsel with Kasowitz, Benson, Torres & Friedman LLP, applies the investigative skills he honed as United States Senator and Attorney General of the State of Connecticut to represent clients in independent and internal investigations and advise them on a wide range of public policy, strategic and regulatory issues. As a seasoned leader who is skilled in the art of facilitating mutually beneficial and strategic agreements, Senator Lieberman also assists corporate clients on tax, health care, security and intellectual property matters. In addition, he counsels clients on international expansion initiatives and business plans.

Prior to joining Kasowitz, Senator Lieberman, the Democratic Vice-Presidential candidate in 2000, served 24 years in the United States Senate, retiring in January 2013 following the end of his fourth term. During his tenure, Senator Lieberman helped shape legislation in virtually every major area of public policy including national and homeland security, foreign policy, fiscal policy, environmental protection, human rights, health care, trade, energy, cybersecurity and taxes. He served in many leadership roles including as Chairman of the Committee on Homeland Security and Government Affairs, which is the Senate's major oversight and investigative committee. On that committee, Senator Lieberman led numerous congressional investigations, including investigations into Enron's collapse, the federal government's response to Hurricane Katrina, the Fort Hood mass shooting, and most recently the deadly attack in Benghazi, Libya. Prior to being elected to the Senate, Senator Lieberman served as the Attorney General of the State of Connecticut for six years. He also served 10 years in the Connecticut State Senate, including three terms as majority leader.

Senator Lieberman is the recipient of numerous awards and recognitions, and in 2012, he received the Ewald von Kleist Award, which is given to the individual who has "made an outstanding contribution to peace and conflict resolution," by the Munich Security Conference, the most prominent independent forum for the exchange of views by international security policy decision-makers. That same year, the Republic of Korea also awarded him the Order of Diplomatic Service Merit Gwanghwa Medal.

In addition to practicing law, Senator Lieberman is a Co-Chair of the American Enterprise Institute's American Internationalism Project, which is a cross-party initiative designed to rebuild and reshape a bipartisan consensus around American global leadership and engagement.



**Loretta E. Lynch** was appointed as U.S. Attorney for the Eastern District of New York by President Obama and entered on duty on May 03, 2010. As U.S. Attorney, she is responsible for overseeing all federal and civil investigations and cases in Brooklyn, Queens, and Staten Island, as well as Nassau and Suffolk Counties on Long Island. She supervises a staff of approximately 170 attorneys and 150 support personnel.

Before joining the U.S. Attorney's office in 1990, Ms. Lynch practiced law as a litigation associate for a leading New York based firm. She began her career in the Eastern District prosecuting narcotics and

violent crime cases. Ms. Lynch served as Chief of the Long Island Office from 1994 to 1998, after serving as the Deputy Chief of General Crimes and as Chief of Intake and Arraignments for the district. While in the Long Island office, she prosecuted white collar crime and public corruption cases, and was the lead prosecutor in a series of trials involving allegations of public corruption in the Long Island town of Brookhaven. Ms. Lynch also served the district as Chief Assistant, where she was a member of the trial team in *United States v. Volpe, et al.*, a five-week civil rights case involving the sexual assault by uniformed New York City police officers upon Haitian immigrant Abner Louima.

President Clinton appointed Ms. Lynch as U.S. Attorney for the EDNY in 1999. From 1999 to 2001, Ms. Lynch was a member of the Attorney General's Advisory Committee, serving as Co-Chair of the White Collar Crime Subcommittee. She was a frequent instructor for the Department of Justice in their Criminal Trial Advocacy Program and served as an Adjunct Professor at St. John's University School of Law.

Before returning to the office as United States Attorney in 2010, Ms. Lynch was a partner in the New York office of Hogan & Hartson, L.L.P. and was a member of the firm's Litigation Group. Her practice focused on commercial litigation, white collar criminal defense, and corporate compliance issues. While at Hogan, Ms. Lynch also served as Special Counsel to the Prosecutor of the ICTR, and conducted a special investigation into allegations of witness tampering and false testimony at the Tribunal.

Ms. Lynch received her A.B., cum laude, from Harvard College in 1981. She received her J.D. from Harvard Law School in 1984, where she was an advisor to the first year moot court competition and a member of the Legal Aid Bureau and Harvard Black Law Student Association.



**Elisa Massimino** was named President and Chief Executive Officer of Human Rights First in September 2008. Human Rights First is one of the nation's leading human rights advocacy organizations. Established in 1978, Human Rights First works in the United States and abroad to promote respect for human rights and the rule of law. As Human Rights First's President and Chief Executive Officer, Ms. Massimino provides overall leadership and strategic direction for the organization and manages its 70 person staff in New York and Washington. Ms. Massimino joined Human Rights First as a staff attorney in 1991 to help establish the Washington office. From 1997 to 2008, she served as the organization's Washington Director. Previously, Ms. Massimino was a litigator in private practice at the Washington law firm of Hogan & Hartson, where she was pro bono counsel in many human rights cases. Before joining the legal profession, she taught philosophy at several universities in Michigan.

Ms. Massimino has a distinguished record of human rights advocacy in Washington. As a national authority on human rights law and policy, she has testified before Congress dozens of times and writes frequently for mainstream publications and specialized journals. She appears regularly in major media outlets and speaks to audiences around the country. She has been quoted in numerous print and online news sources, including: The New York Times, The

Washington Post and other global publications, and she has been featured on ABC News, NBC Dateline, The NewsHour with Jim Lehrer, BBC and many other news outlets.

The daughter of a nuclear submarine commander, Massimino was instrumental in a recent effort to assemble a group of retired generals and admirals to speak out publicly against policies authorizing the torture of prisoners in U.S. custody. This coalition of military leaders has played a pivotal role in the effort to restore compliance with the Geneva Conventions standard for treatment of prisoners. Ms. Massimino holds a J.D. from the University of Michigan where she was an Editor of the Journal of Law Reform. She holds an M.A. in philosophy from Johns Hopkins University, and is a Phi Beta Kappa graduate of Trinity University in San Antonio, Texas. Massimino serves as an adjunct professor at Georgetown University Law Center, where she teaches human rights advocacy, and has taught international human rights law at the University of Virginia and refugee law at the George Washington University School of Law. She is a member of the bar of the United States Supreme Court.



**Jacquelyn Matava**, mezzo soprano, a native of Farmington, CT, received her Bachelor of Arts cum laude from Vassar College with majors in both music and economics, and her Master of Music in vocal performance from the Jacobs School of Music, where she is also completing doctoral studies. During her tenure at IU, Jacquelyn has performed several roles with the IU Opera Theater, including Charlotte in Massenet's *Werther*, the title role in Massenet's *Cendrillon*, Nancy in Britten's *Albert Herring*, Marthe in Gounod's *Faust*, and Cecilia March in Adamo's *Little Women*. As a 2014 Apprentice Artist with Opera Saratoga, she will sing Second Lady in Mozart's *Die Zauberflöte* and be featured in a workshop performance of *Roscoe*, a new opera by Evan Mack.



**Douglass B. Maynard** was appointed the New York City Police Department's Deputy Commissioner for Legal Matters in January 2013.

A former partner at Akin Gump Strauss Hauer & Feld and co-head of its New York litigation section, Deputy Commissioner Maynard also served as Associate General Counsel at Time Inc., and before that as Assistant United States Attorney for the Southern District of New York. As Assistant U.S. Attorney from 1990 to 1996, Mr. Maynard was the federal prosecutor responsible for the investigation and prosecution of a wide range of federal crimes including RICO violations, narcotics trafficking, bank fraud and mail and wire fraud. He investigated and prosecuted a number of major Russian organized crime cases, then an emerging and international crime problem. Those cases involved murder, extortion, drug trafficking and other crimes in the United States, Europe, and Asia. As part of that effort, he coordinated with European law enforcement officials to extradite defendants from Italy, Romania, Austria and Denmark.

In private practice he focused on white collar criminal and regulatory defense, and also represented magazine and book publishers and news organizations in libel and other media-related litigation. Before joining the Justice Department, he was an associate at Patterson,

Belknap, Webb & Tyler between 1986 and 1990. Deputy Commissioner Maynard is a 1982 graduate of Yale University, and he received his J.D. from New York University in 1986. In his new post, Deputy Commissioner Maynard will oversee a staff of 150 civilian and uniformed members of the service, including 75 lawyers. He succeeds S. Andrew Schaffer, who retired.

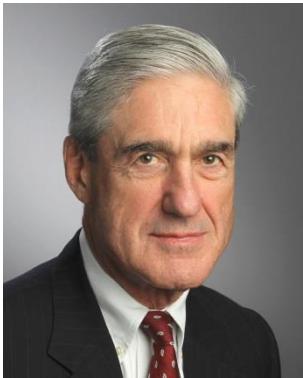


**Roslynn R. Mauskopf** was appointed United States District Judge for the Eastern District of New York on October 18, 2007, and entered on duty on October 19, 2007.

Judge Mauskopf has spent her entire career in public service. From August 1982 to October 1995, Judge Mauskopf served as an Assistant District Attorney under Robert M. Morgenthau, the Manhattan District Attorney. She served in both the Trial and Investigations Divisions, and was promoted in 1992 to Deputy Chief of the Special Prosecutions Bureau, and again in 1993 to Chief of the Frauds Bureau. In 1995, Judge Mauskopf was appointed by Governor George E. Pataki as the New York State Inspector General. In that capacity, she led the statewide, independent office responsible for investigating allegations of corruption, fraud, criminal activity, conflicts of interest and abuse in Executive Branch agencies. Beginning in 1999 and concurrent with her continued service as Inspector General, Judge Mauskopf served as Chair of the Governor's Moreland Act Commission on New York City Schools, an investigative panel that uncovered systemic abuses in the operations and fiscal affairs of the New York City Board of Education and the New York City School Construction Authority.

In September 2002, Judge Mauskopf was appointed by President George W. Bush as United States Attorney for the Eastern District of New York, a position she held until her judicial appointment. She was selected to serve on the President's Corporate Fraud Task Force, the Attorney General's Advisory Committee, and the Department of Justice's Executive Working Group, which serves as liaison to the nation's Attorneys General and District Attorneys. She also served on Department policy committees in the areas of Civil Rights, Violent and Organized Crime, Sentencing, and Management and Budget.

Judge Mauskopf graduated from Brandeis University in 1979, and earned her law degree from Georgetown University Law Center in 1982. A native of Washington, D.C., she is the daughter of Czech holocaust survivors who immigrated to America and established a small neighborhood grocery store which they operated for more than 40 years.



**Robert S. Mueller, III** is a partner at Wilmer Cutler Pickering Hale and Dorr LLP in Washington, DC, where his practice focuses on investigations, crisis management, privacy and cyber security work. Mr. Mueller was sworn in as Director of the FBI by President George W. Bush on September 4, 2001 – just one week before 9/11. His ten-year term was extended for an additional two years at the request of President Barack Obama and pursuant to legislation passed by Congress.

He graduated from Princeton University in 1966 and earned an M.A. in International Relations at New York University in 1967. Mr. Mueller earned a J.D. from the University of Virginia Law School in 1973 where he served on the Law Review. After college, he joined the United States Marine Corps, where he served as an officer for three years, leading a rifle platoon of the Third Marine Division in Vietnam. He is the recipient of the Bronze Star, two Navy Commendation Medals, the Purple Heart and the Vietnamese Cross of Gallantry.

Mr. Mueller worked as a litigator in San Francisco until 1976. He then served for 12 years in the United States Attorney's Offices, first in the Northern District of California in San Francisco, where he rose to be chief of its criminal division. In 1982, he moved to Boston as an Assistant United States Attorney where he investigated and prosecuted major financial fraud, terrorist and public corruption cases, as well as narcotics conspiracies and international money launderers.

After serving as a partner at the Boston law firm of Hill and Barlow, Mr. Mueller returned to public service. In 1989, he served in the United States Department of Justice as an assistant to Attorney General Richard L. Thornburgh. The following year he took charge of its Criminal Division, where he oversaw prosecutions including the conviction of Panama leader Manuel Noriega, the Lockerbie Pan Am 103 bombing case and the John Gotti mobster prosecution. In 1991, he was elected Fellow of the American College of Trial Lawyers.

In 1993, Mr. Mueller became a partner at Boston's Hale and Dorr, specializing in complex white collar crime litigation. He returned to public service in 1995 as senior litigator in the Homicide Section of the District of Columbia United States Attorney's Office. In 1998, Mr. Mueller was named United States Attorney in San Francisco and held that position until 2001. He then served as Acting Deputy Attorney General of the United States Department of Justice for several months before becoming FBI Director.



**Michael B. Mukasey** served as Attorney General of the United States, the nation's chief law enforcement officer from November 2007 to January 2009. He oversaw the U.S. Department of Justice and advised on critical issues of domestic and international law. Judge Mukasey joined Debevoise & Plimpton LLP as a partner in the litigation practice in New York in February 2009, focusing his practice primarily on internal investigations, independent board reviews and corporate governance.

From 1988 to 2006, Judge Mukasey served as a district judge in the United States District Court for the Southern District of New York, becoming Chief Judge in 2000. He presided over many significant cases including: the terrorism trial of Omar Abdel Rahman (the "Blind Sheik") and nine other defendants; *SR Int'l Bus. Ins. Co. v. World Trade Ctr. Props, LLC*, addressing whether the two-plane attack on the World Trade Center constituted one or two "occurrences" for insurance purposes; and *Padilla v. Rumsfeld*, addressing the detention of a citizen suspected of engaging in terrorism against the United States.

From 1972 to 1976, Judge Mukasey served as an Assistant United States Attorney for the Southern District of New York, and as Chief of the Official Corruption Unit from 1975 to 1976. His practice consisted of criminal litigation on behalf of the government, including investigation and prosecution of narcotics, bank robbery, interstate theft, securities fraud, fraud on the government and bribery. From 1976 to 1987 and from 2006 to 2007, he was in private practice.

Judge Mukasey has received numerous honors, including the Federal Bar Council's Learned Hand Medal for Excellence in Federal Jurisprudence. He served as Chairman of the Committee on Public Access to Information and Proceedings of the New York Bar Association from 1984 to 1987. He served on the Federal Courts Committee of the Association of the Bar of the City of New York from 1979 to 1982 and its Communications Law Committee from 1983 to 1986. Judge Mukasey was also a part-time lecturer at Columbia School of Law from January 1993 to May 2007, teaching trial advocacy.

He received his LL.B. from Yale Law School in 1967 and his B.A. from Columbia College in 1963.



**Janet Napolitano** was named the 20th president of the University of California on July 18, 2013, and took office on September 30, 2013. She leads a university system with 10 campuses, five medical centers, three affiliated national laboratories, and a statewide agriculture and natural resources program.

Ms. Napolitano is a distinguished public servant with a record of leading large, complex organizations at the federal and state levels. She served as Secretary of Homeland Security from 2009-2013, as Governor of Arizona from 2003-2009, as Attorney General of Arizona from 1998-2003, and as U.S. Attorney for the District of Arizona from 1993-1997. Before that, she practiced at the law firm of Lewis & Roca in Phoenix, where she became a partner in 1989. She began her career in 1983 as a law clerk for Judge Mary M. Schroeder of the U.S. Court of Appeals for the Ninth Circuit. As Governor of Arizona, Ms. Napolitano focused on education, from pre-kindergarten through

public higher education. She was the first woman to chair the National Governors Association, and was named one of the nation's top five governors by Time magazine.

Ms. Napolitano earned a B.A. degree (summa cum laude in Political Science) in 1979 from Santa Clara University, where she was Phi Beta Kappa, a Truman Scholar and the university's first female valedictorian. She received her J.D. in 1983 from the University of Virginia School of Law. Napolitano holds honorary degrees from several universities and colleges, including Santa Clara University, Emory University and Pomona College. In 2010, she was awarded the prestigious Thomas Jefferson Foundation Medal (Law), the University of Virginia's highest external honor.



**Faiza Patel** serves as Co-Director of the Brennan Center's Liberty and National Security Program. She has testified before Congress opposing the dragnet surveillance of Muslims, organized advocacy efforts against state laws designed to incite fear of Islam, and developed legislation creating an independent Inspector General for the NYPD. Ms. Patel is the author of three reports: *Foreign Law Bans: Legal Uncertainties and Practical Problems*, *A Proposal for an NYPD Inspector General*, and *Rethinking Radicalization*. She is also a frequent commentator on national security and counterterrorism issues for media outlets such as The New York Times, The Washington Post, The Economist, The Guardian, MSNBC, Al-Jazeera, NPR, New York Daily News, and The National Law Journal. Before joining the Brennan Center, Ms. Patel worked as a senior policy officer at the Organization for the Prohibition of Chemical Weapons in The Hague, and clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Born and raised in Pakistan, Ms. Patel is a graduate of Harvard College and the NYU School of Law.



**Samuel Rascoff** is an emerging leader in the field of national security law. He teaches and writes in the area, and serves as faculty director of the Center on Law and Security at the NYU School of Law. Named a Carnegie Scholar in 2009, Professor Rascoff came to the NYU School of Law from the New York City Police Department, where, as Director of Intelligence Analysis, he created and led a team responsible for assessing the terrorist threat to the city. A graduate of Harvard summa cum laude, Oxford with first-class honors, and Yale Law School. Professor Rascoff previously served as a law clerk to Judge Pierre N. Leval of the U.S. Court of Appeals for the Second Circuit and Justice David H. Souter of the U.S. Supreme Court. He was also a special assistant with the Coalition Provisional Authority in Iraq and an associate at Wachtell, Lipton, Rosen & Katz. His recent publications include "Deterring Terror" (forthcoming, New York University Law Review), "Establishing Official Islam? The Law and Strategy of Counter-Radicalization" (Stanford Law Review), "Domesticating Intelligence" (Southern California Law Review), and "The Law of Homegrown (Counter)Terrorism" (Texas Law Review).



**David Raskin**, a former federal prosecutor with significant expertise in the area of national and global security, is a New York-based partner in the international law firm Clifford Chance. Mr. Raskin represents companies and individuals in matters before the Department of Justice and other federal, state and local agencies. He specializes in conducting multijurisdictional internal investigations.

Prior to joining Clifford Chance, Mr. Raskin served for more than 12 years as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York. For many of those years, he was a chief of the Office's terrorism unit, supervising a comprehensive docket of the country's most significant national security investigations and prosecutions. In addition, notably, Mr. Raskin prosecuted Zacarias Moussaoui for conspiring to carry out the terrorist attacks of September 11, 2001; led the Department of Justice's investigation of Khalid Sheikh Mohammed, and other Guantánamo Bay detainees, for their leading roles in that conspiracy; argued the appeal of three al Qaeda operatives convicted for the bombings of U.S. embassies in Tanzania and Kenya; and was lead trial counsel in the prosecution of James Cromitie and others for conspiring to bomb military and religious targets in New York City. Mr. Raskin also investigated and prosecuted numerous cases involving violent organized crime and led a global bribery investigation that resulted in the December 2011 indictment of former executives of Siemens AG. For his government service, Mr. Raskin received two Attorney General Awards from the Department of Justice and the New York City Bar Association's Henry L. Stimson Medal for outstanding contributions to the Office of the United States Attorney.

Mr. Raskin is a graduate of New York Law School, magna cum laude, where he served as Executive Articles Editor on the Law Review. He was a law clerk to the Honorable Leonard D. Wexler, United States District Judge for the Eastern District of New York. Mr. Raskin is a Lecturer-in-Law at Columbia Law School and an Adjunct Professor at New York Law School.



**Richard Salgado** serves as Google's Director for law enforcement and information security matters. Richard oversees Google's worldwide law enforcement efforts, and legal matters relating to data security and investigations. Prior to joining Google, Mr. Salgado was with Yahoo!, focusing on international security and law enforcement compliance work. He also served as senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. As a federal prosecutor, he specialized in investigating and prosecuting computer network cases, such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other technology driven privacy crimes. In 2005, he joined

Stanford Law School as a legal lecturer on computer crime, Internet business legal and policy issues, and modern surveillance law. He previously served as an adjunct law professor at Georgetown University Law Center and George Mason Law School, and as a faculty member of the National Judicial College. Mr. Salgado is a senior instructor with the SANS Institute, teaching on the legal issues in computer forensics and network investigations. He received his J.D. from Yale Law School.



**Randy L. Shapiro** joined Bloomberg L.P. as Global Media Counsel of Bloomberg News in August 2013. She is the newsroom lawyer to more than 2400 journalists around the globe and is responsible for newsgathering advice and prepublication review, FOIA and access requests, and newsroom legal training. Prior to joining Bloomberg, Randy was the Chief Administrative Officer and General Counsel of The Newsweek/Daily Beast Company, the product of a 2010 merger between Newsweek magazine and The Daily Beast website. There, she had oversight of all legal matters including: prepublication review of editorial content; libel and privacy advice and training; copyright analysis, licensing and protection; global labor and employment counseling; contracts; and trademark and domain name registrations. Prior to joining Newsweek in 1998 as Assistant Counsel, Ms. Shapiro was a commercial litigator with Stroock & Stroock & Lavan, where she was a member of the team representing The New York Post, as well as the associate liaison to the firm's Pro Bono Committee.

Ms. Shapiro is currently Co-Chair of the Mentoring Committee of the New York Women's Bar Association, and is a member of the Committee on Communications and Media Law of the Association of the Bar of the City of New York, and the Forum on Communication Law of the American Bar Association.

Ms. Shapiro earned her law degree from Boston University School of Law, and received a Bachelor of Arts degree in Spanish and Economics from Tufts University. She resides in Manhattan with her husband and two sons.



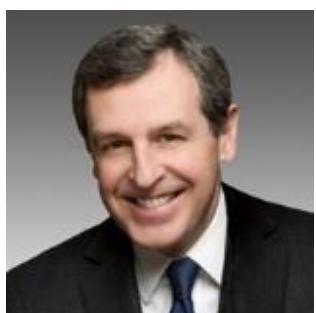
**David Snively** is Executive Vice President, Secretary and General Counsel for St. Louis-based Monsanto Company (NYSE: MON), the world's largest seed company and leader in agricultural biotechnology. As a senior member of Monsanto's international executive team he leads its legal and environmental, safety and health functions supporting the company's effort to help farmers meet the challenges of producing more food, conserving precious natural resources and improving lives via sustainable agriculture. Previously selected by Corporate Board Member Magazine as "America's Top General Counsel" and among "America's 50 Outstanding General Counsel" by The National Law Journal, Snively has played a leading role at Monsanto on intellectual property, biotechnology strategy, antitrust, crisis response, governance and public policy issues. In 2013, Financial Times recognized Monsanto and Google as "2013's Most Innovative Law Departments" and Forbes listed the company 34th among "The World's Most Innovative Companies." Managing IP Magazine in 2014 honored Monsanto as "In House IP Department of the Year" and for "Milestone IP Case of the Year (Bowman)".

Trained as a trial lawyer with Barnes & Thornburg, at Monsanto he has directed many notable cases including the longest civil jury trial in U.S. history (3 ½ years), *In re Agent Orange*, a verdict for \$1B in a patent trial win against DuPont and the unanimous Supreme Court decision in *Bowman* upholding intellectual property concepts central to the licensing of the company's

technology. He holds a Bachelor of Science degree from Ball State University and a J.D. from Indiana University.



**George Ross Somerville**, tenor, from Point Pleasant, New Jersey, has appeared with Sarasota Opera, Opera Theatre of Saint Louis, Des Moines Metro Opera, Opera Philadelphia, The Princeton Festival, CoOperative Concert Opera, and Opera Slavica. A 2014 Apprentice Artist with Opera Saratoga, he will sing First Armored Man in *Die Zauberflöte* and premiere the role of Alex Fitzgibbon in a workshop performance of Evan Mack's new opera, *Roscoe*. He is on the full chorus roster of Opera Philadelphia, and he is a member of the Extra Chorus with the Metropolitan Opera.



**Edward M. Stroz** founded Stroz Friedberg in 2000, serving first as Co-President and currently as Executive Chairman. His work includes responding to Internet extortions, denial of service attacks, computer hacking, insider abuse, theft of trade secrets, electronic discovery matters, and providing expert testimony.

Mr. Stroz has pioneered the use of behavioral science in the investigative methodology to gain insights about the intent and state-of-mind of computer users. He has co-authored a book on the threats of computer crime and abuse posed by insiders and testified numerous times in court and at depositions as an expert witness. He has supervised hundreds of forensic assignments in assisting corporate clients, trial counsel, and individuals, and has conducted security assessments for major public and private entities. As a Special Agent at the FBI, Mr. Stroz was responsible for the formation of the FBI's Computer Crime Squad in New York City, where he supervised investigations involving computer intrusions, denial of service attacks, illegal Internet wiretapping, fraud, and violations of intellectual property rights, including trade secrets. In addition to his many high-profile cases, Mr. Stroz led his squad, together with the National Security Agency (NSA) and other agencies, as participants in the war game exercise called "Eligible Receiver."

Earlier in his FBI career, Mr. Stroz successfully investigated major financial crimes, including dozens of bank frauds in west Texas; bank fraud and money laundering committed by the CEO of Arochem Corporation stemming from a \$196 million oil-trading scheme; kickback schemes in the stock market by running an undercover stock brokerage firm; and a \$1.1 billion fraud scheme at Daiwa Bank in New York.

Mr. Stroz is on the Board of Trustees of Fordham University, and an advisor to the Center on Law and Information Policy (CLIP) at Fordham Law School. He serves on the New York State Courts System E-Discovery Working Group, established to provide ongoing support and expertise to the New York State Judiciary in the area of e-discovery.

He served as Co-Chair on the Planning Committee for the International Conference on Cyber Security (ICCS 2012) organized with the FBI at Fordham University, and attended by investigators from over 40 countries.

Trained as a Certified Public Accountant, Mr. Stroz is a member of the American Institute, and the New York State Society of Certified Public Accountants, as well as the International Association for Identification.



**Richard J. Sullivan** was sworn in as a United States District Judge for the Southern District of New York in August 2007. Prior to becoming a judge, he served as the General Counsel and Managing Director of Marsh Inc., the world's leading risk and insurance services firm. From 1994 to 2005, he served as an Assistant United States Attorney in the Southern District of New York, where he was Chief of the International Narcotics Trafficking Unit and Director of the New York/New Jersey Organized Crime Drug Enforcement Task Force. In 2003, he was awarded the Henry L. Stimson Medal from the Association of the Bar of the City of New York. In 1998, he was named the Federal Law Enforcement Association's Prosecutor of the Year. Prior to joining the U.S. Attorney's Office, he was a litigation associate at Wachtell, Lipton, Rosen & Katz in New York and a law clerk to the Honorable David M. Ebel of the United States Court of Appeals for the 10th Circuit. He is a graduate of Yale Law School, the College of William & Mary, and Chaminade High School on Long Island. From 1986 to 1987, he served as a New York City Urban Fellow under New York City Police Commissioner Benjamin Ward. Judge Sullivan is on the executive board of the New York American Inn of Court and is an adjunct professor at Columbia Law School, where he teaches a course on sentencing, and at Fordham Law School, where he teaches courses on white collar crime and trial advocacy and was named Adjunct Professor of the Year.



**Dina Temple-Raston**, a member of NPR's national security team, reports about counterterrorism at home and abroad for NPR News. Her reporting can be heard on NPR's newsmagazines. She joined NPR in March 2007.

Prior to NPR, Ms. Temple-Raston was a longtime foreign correspondent for Bloomberg News in Asia. She opened Bloomberg's Shanghai and Hong Kong offices and worked for Bloomberg's financial wire and radio operations. She also served as Bloomberg News' White House correspondent during the Clinton administration and covered financial markets and economics for both USA Today and CNNfn.

Ms. Temple-Raston is an award-winning author. Her first book concerning race in America, entitled *A Death in Texas*, won the Barnes' and Noble Discover Award and was chosen as one of The Washington Post's Best Books of 2002. Her second book, *Justice on the Grass*, about the role Radio Mille Collines played in fomenting the Rwandan genocide, was a Foreign Affairs magazine bestseller. Her more recent two books relate to civil liberties and national security. The first, *In Defense of Our America* (Harper Collins) coauthored with Anthony D. Romero, Executive

Director of the ACLU, looks at civil liberties in post-9/11 America. The other explores America's first so-called "sleeper cell," the Lackawanna Six, and the issues that face Muslims in America. It is entitled *The Jihad Next Door*.

Ms. Temple-Raston holds a B.A. from Northwestern University and an M.A. from Columbia University School of Journalism. She has an honorary doctorate from Manhattanville College.



**John Thorne** is a partner with Kellogg, Huber, Hansen, Todd, Evans & Figel, PLLC, in Washington, DC. He represents tech companies in antitrust, intellectual property, and commercial litigation.

From 2000 to 2012, Mr. Thorne was senior vice president and deputy general counsel at Verizon Communications Inc. where he headed Verizon's competition and intellectual property groups. Global Counsel Awards named his IP group one of the top five in the world in 2008 and 2010, and named his IP group the best in the world in 2011. Global Counsel Awards named him the best corporate competition lawyer in the world in 2009.

Mr. Thorne is a co-author of the principal telecom law treatises and numerous articles on antitrust. He taught telecom law for ten years at Columbia Law School and for two years at Georgetown University Law Center.

Mr. Thorne graduated summa cum laude in three years from Kenyon College with high honors in mathematics. He graduated Order of the Coif and was the law review articles editor at Northwestern University Law School. He clerked for Hon. Walter J. Cummings, Chief Judge of the U.S. Court of Appeals for the Seventh Circuit.

Mr. Thorne is a member of the Illinois and District of Columbia bars, and the bars of the U.S. Supreme Court, and the D.C., Federal, Second, Fifth, Seventh, and Ninth Circuits.



**Derrick Wang** is a composer, lyricist, and pianist, creating dramatic music for an interdisciplinary world. He also engages audiences as a speaker on music, law, and the future of the performing arts. His compositions have received national and international honors, including awards from America's two major performing-rights organizations, ASCAP (the American Society of Composers, Authors, and Publishers) and BMI (Broadcast Music, Inc.). His work has been performed both in the United States and abroad, in venues such as Beijing's Forbidden City Concert Hall and the Shanghai Grand Theatre in the run-up to the 2008 Olympics. In addition, he has arranged music for Marvin Hamlisch, the Leonard Bernstein Office, and The New York Pops at Carnegie Hall.

He is the creator of the opera *Scalia/Ginsburg*, about Supreme Court Justices Antonin Scalia and Ruth Bader Ginsburg. *Scalia/Ginsburg* was introduced in June 2013 at the Supreme Court of the United States by NPR's Nina Totenberg, with further coverage by the Associated Press,

Bloomberg, The Washington Post, and the ABA Journal. Further development of the opera has included a staged reading by the Maryland Opera Studio (February 2014) and a staged presentation of excerpts by the Washington National Opera at the Smithsonian (April 2014). Other performances this season include the Canadian premiere of his Valley, Mountain, Sky by the Winnipeg Symphony Orchestra (April 2014).

He received his A.B. in Music, Phi Beta Kappa, magna cum laude, from Harvard University; his M.M. in Composition on a Richardson Scholarship from the Yale School of Music; and his J.D. on a Houff Leadership Scholarship from the University of Maryland Carey School of Law.



**Matthew C. Waxman** is Professor of Law at Columbia Law School, where he specializes in national security law and international law. He is also Adjunct Senior Fellow for Law & Foreign Policy at the Council on Foreign Relations and a member of the Hoover Institution Task Force on National Security and Law. Prof. Waxman previously served at the U.S. Department of State, as Principal Deputy Director and Acting Director of the Secretary of State's Policy Planning Staff. His prior government appointments included Deputy Assistant Secretary of Defense for Detainee Affairs, Director for Contingency Planning & International Justice at the National Security Council, and special assistant to National Security Advisor Condoleezza Rice. He is a graduate of Yale College and Yale Law School, and studied international relations as a Fulbright Scholar in the United Kingdom. After law school, he served as a law clerk to Supreme Court Justice David H. Souter and U.S. Court of Appeals Judge Joel M. Flaum. Earlier in his career, Mr. Waxman worked as a defense analyst at RAND.



**Andrew Weissmann** is a Senior Fellow to both the Center for Law and Security and the Center on the Administration of Criminal Law.

Mr. Weissmann served as the General Counsel for the Federal Bureau of Investigation from 2011 to 2013. He previously served as special counsel to Director Mueller in 2005, after which he was a partner at Jenner & Block LLP in New York City. From 2002-2005, he served as Deputy and then Director of the Enron Task Force in Washington, D.C., where he supervised the prosecution of more than 30 individuals in connection with the company's collapse. Mr. Weissmann was a federal prosecutor for 15 years in the Eastern District of New York, where he served as Chief of the Criminal Division. He prosecuted numerous members of the Colombo, Gambino, and Genovese families, including the bosses of the Colombo and Genovese families. Mr. Weissmann has extensive experience in private practice. Mr. Weissmann won the largest Financial Industry Regulatory Authority arbitration award in history. He has taught criminal law and procedure at Fordham Law School and Brooklyn Law School. He holds a Juris Doctor degree from Columbia Law School and was on the managing board of the Columbia Law Review. He has a Bachelor of Arts degree from Princeton University and attended the University of Geneva on a Fulbright Fellowship.

## **Appendix B: Remarks of Justice Ginsburg, June 13, 2014**

Because the Second Circuit held no Judicial Conference last year, I will include in these remarks descriptions of Supreme Court decisions from last term (2012-2013) as well as the (2013-2014) term still underway. About the same number of cases were fully briefed and argued both terms, 73 last term, 70 in the current term. Last term's decisions swelled to 78, because we decided five cases per curiam, without full briefing and with no oral argument. This year, we have so far decided five cases that summary way.

Last term, as usual, our unanimity rate was high. We agreed, at least on the bottom line judgment, in 38 of the 78 decisions handed down. In contrast to that 49% agreement rate, we divided 5 to 4 (or 5 to 3 with one justice recused) in 23 of the post-argument dispositions, a sharp disagreement rate just above 30%. This term, we have so far unanimously agreed on the bottom-line judgment in 46% of the argued cases plus unanimous *per curiam* dispositions. Five to four divisions were returned in 10% of total argued cases, a disagreement rate likely to increase in the term's final weeks. In short, although not broadcast in the media, we agree much more often than we disagree. That is notable, I think, because we tend to grant review only when other courts have divided on the answer to the issue we take up.

Highest agreement rate, 2012-2013, Justice Kagan and me. We were together in 96% of the cases on which both of us voted. Highest disagreement rate last term, Justice Alito and me, agreeing in 45 of the 77 cases in which both of us participated. Most likely to appear in the majority, for the fifth consecutive term, Justice Kennedy, voting with the majority last term in 91% of the decisions handed down. Least likely to appear in the majority last term, Justice Scalia, voting with the majority in 78% of the total decisions rendered. Most active at oral argument 2012-2013, Justice Sotomayor outran Justice Scalia. Her average number of questions per argument, 21.6, Justice Scalia's, 20.5. It is too soon to report similar information for the current Term.

Honing in on the Second Circuit, last term we granted review in ten cases from the Circuit, reversing six and affirming four. Most attention garnering among the ten, *United States v. Windsor*. This term, we granted review in only five cases from the Circuit, so far affirming two and reversing one that drew headlines, *Town of Greece v. Galloway*. I will say more about *Windsor* and *Town of Greece* later in this account of the 2012 and 2013 terms.

Some other cases of large importance. With an eye on the clock, I will describe them in short order. *Shelby County v. Holder*, decided the final week of the 2012-2013 term. In that 5 to 4 decision, the Court invalidated the Voting Rights Act's coverage formula, the mechanism used to identify which state and local governments had to seek federal preclearance before altering their election laws. I wrote for the dissenters. By overwhelming majorities in both Houses, and based on a voluminous record, Congress had renewed the Voting Rights Act's coverage formula unchanged. The dissent explains why four of us thought the Court should have accorded greater respect for the judgment of the Political Branches. Like the currently leading

campaign finance decision, *Citizens United v. Federal Election Commission*, I regard *Shelby County* as an egregiously wrong decision that should not have staying power.

Among headline cases from the current term are *Sebelius v. Hobby Lobby Stores* and *Conestoga Wood Specialties Corp. v. Sebelius*, cases brought by for-profit corporations challenging the Affordable Care Act's so-called contraceptive mandate. The corporations, both commercial enterprises, assert a right under the Free Exercise Clause of the First Amendment, and the Religious Freedom Restoration Act, to refuse to cover under their health insurance plans certain contraceptives—specifically, IUDs and morning and week after pills. The question presented: Can Congress lawfully confine exemptions from contraceptive coverage to churches and nonprofit religion-oriented organizations? The Tenth Circuit ruled in favor of the corporation; the Third Circuit upheld the law as Congress wrote it. The Court's decision will be among the last released this month.

I should mention too *NLRB v. Noel Canning*, a case from the D. C. Circuit, argued in January and still awaiting decision. At issue, the President's authority to make recess appointments. The questions presented: May the power be exercised during an interim break, or only during an end-of-session recess? Must the vacancy arise during the recess or may it already exist prior to the recess? Finally, does a period count as a recess when the Senate convenes every three days in pro forma sessions?

Next, I will concentrate, although not exclusively, on cases coming to us from the Second Circuit, and describe them less summarily. We heard the first day of the 2012-2013 term, *Kiobel v. Royal Dutch Petroleum Co.* *Kiobel* was initially argued the preceding term. The petitioner had asked the Court to resolve this question: Are corporations amenable to suit under the Alien Tort Statute, a law on the books since 1789, authorizing suit in federal court by an alien for a tort "committed in violation of the law of nations"? (The "law of nations," a term appearing in Article I, §8 of the Constitution, is what we today call "international law.") A panel of this Circuit had answered: Suit under the Act lies only against individuals; corporations are not covered.

On brief and at the initial argument, the respondent corporations proposed an alternative ground for affirmance: The Alien Tort Statute, they contended, should not apply offshore, that is, to conduct occurring in a foreign nation. The claim in *Kiobel* was that three oil companies with operations in Nigeria, all three headquartered abroad, had aided and abetted the Nigerian military's gross human rights violations. Plaintiffs in the case were victims, or the survivors of victims, of the alleged atrocities. Inviting full briefing on the alternative theory, the Court set the case for reargument in October 2012.

Writing for the majority, the Chief Justice did not address the corporate liability question resolved by the Second Circuit, the question on which review initially had been granted. Instead, the Chief embraced the presumption against extraterritorial application of domestic laws. Under that presumption, the Court held, the plaintiffs' claims could not be entertained because "all . . . relevant conduct took place outside the United States." The Court added that "even where the [plaintiffs'] claims touch and concern the territory of the United States, they must do so with sufficient force to displace the presumption against extraterritorial application."

Justice Breyer, joined by Justices Sotomayor, Kagan, and me, agreed with the majority's bottom line, but not with the potential breadth of the Court's reasoning. *Kiobel*, Justice Breyer acknowledged, did not belong in a U.S. court, for nothing linked the case to this country. But rather than announcing a sweeping presumption against extraterritoriality, Justice Breyer invoked "principles and practices of foreign relations law." Jurisdiction would lie under the Alien Tort Statute, he maintained, when "the defendant's conduct substantially and adversely affects an important American national interest." One such interest, he identified, was ensuring that the United States would not become "a safe harbor . . . for a torturer or other common enemy of mankind." Thus, if a human rights violator acted abroad against foreign nationals and later shows up in the United States, Justice Breyer urged, the victims could sue him here. The Second Circuit so held in the famous *Filartiga* case. It remains to be seen whether a majority will uphold *Filartiga* should the issue come before us.

*Kirtsaeng v. John Wiley & Sons, Inc.*, another Second Circuit decision the Court took up last term, involved a clash between copyright owners and proponents of less restrictive access to printed works. The question presented: Does the U.S. Copyright Act empower a copyright owner to bar the importation of a copy of her work lawfully manufactured and sold abroad? The petitioner in the case, Supap Kirtsaeng, was an enterprising foreign student taking courses at universities in the United States. Seeing a business opportunity, he imported low-priced textbooks from his native Thailand, enlisting his relatives in Thailand to buy the books there. He then resold the books for a profit in the United States. The textbooks' publisher sued Kirtsaeng for copyright infringement, invoking a provision of the Copyright Act, 17 U. S. C. §602(a)(1), that provides: "Importation into the United States, without the authority of the [copyright] owner . . . , of copies . . . of a work . . . acquired outside the United States is an infringement of the exclusive right to distribute copies."

In an opinion written by Justice Breyer, the Court ruled in favor of Kirtsaeng, overturning the \$600,000 judgment the District Court had entered against him and reversing the decision of the Second Circuit. Kirtsaeng's importations, the Court held, were permitted by the "first sale doctrine." That doctrine allows the "owner of a particular copy" of a copyrighted work "to sell or otherwise dispose of . . . that copy" without first obtaining the copyright owner's permission. As statutorily codified, the first-sale doctrine applies only to copies "lawfully made under this title"—that is, Title 17, the Copyright Title of the U. S. Code. The textbooks Kirtsaeng imported satisfied this requirement, the Court said, because they had been "manufactured abroad with the permission of the copyright owner," thus they were "lawfully made."

I sided with the Second Circuit and dissented in an opinion joined by Justice Kennedy in full and by Justice Scalia in part. If "lawfully made" was key to the Court's decision, "under this title" was critical to the dissent. The phrase "lawfully made under this title," as I read it, refers to copies whose creation is governed, not by foreign law, but by Title 17 of the U. S. Code. And that meant made in the U.S.A., because the U. S. Copyright Act does not apply extraterritorially. The foreign-manufactured textbooks Kirtsaeng imported, though lawfully made in Thailand in accord with Thai law, were, in the dissent's view, not "lawfully made under [Title 17]," the crucial precondition for application of the codified first-sale doctrine. That reading would have avoided "shrink[ing] to insignificance" the copyright protection Congress provided against the unauthorized importation of foreign-made copies.

Last term, the Court heard only one First Amendment case, and it came to us from the Second Circuit, *Agency for International Development v. Alliance for Open Society International*. That case involved a condition Congress placed on federal funding for non-governmental organizations that endeavor to assist in combatting HIV/AIDS. Finding that the commercial sex industry contributed to the spread of HIV/AIDS, Congress barred federal funding “to any group or organization that does not have a policy explicitly opposing prostitution and sex trafficking.” I will call this prohibition the “Policy Requirement.”

A group of domestic organizations engaged in efforts to combat HIV/AIDS overseas sued, arguing that the Policy Requirement violated their First Amendment rights. The organizations were not proponents of prostitution, but they feared that the Policy Requirement would make it more difficult for them to work with prostitutes to curtail the spread of HIV/AIDS. On review, a panel of the Second Circuit held that the Policy Requirement was an unconstitutional restriction on speech.

In an opinion written by Chief Justice Roberts, joined by Justices Kennedy, Breyer, Alito, Sotomayor, and me, the Court agreed with the Second Circuit. The government may set conditions that define the limits of a government spending program, we explained, but it may not leverage funding to regulate a fund recipient’s speech outside the funded program. Demanding that organizations spout the government’s position opposing prostitution and sex trafficking, we held, reached beyond the funded program in curtailing recipients’ activities.

In dissent, Justice Scalia (joined by Justice Thomas) viewed the Policy Requirement as an appropriate means to identify organizations that would make fit partners for the fight against HIV/AIDS. The condition, Justice Scalia wrote, was “the reasonable price of admission” to the government spending program. An organization’s speech was not compelled, in his view, for the organization could choose to accept or reject the government’s condition (and the money that came with it) as the organization saw fit.

On the very last opinion-announcing day of the 2012-2013 term, June 26, the Court released decisions in the two same-sex marriage cases heard in tandem in March 2013. I will summarize the first announced, *United States v. Windsor*, which, as I noted earlier, came to us from the Second Circuit. The case presented a challenge to the constitutionality of §3 of the Defense of Marriage Act, or DOMA. Section 3 defined the term “marriage,” for all federal law purposes, as “only a legal union between one man and one woman.” Under this definition, same-sex couples, married lawfully under state law, were not recognized as married by the federal government. In all the ways in which a marital relationship matters for federal purposes—from social security benefits and taxation to joint burial privileges in veterans’ cemeteries—DOMA treated these couples as unrelated persons.

The plaintiff in the case, Edith Windsor, married her partner of some 40 years, Thea Spyer, in Canada in 2007. The couple’s state of residence—New York—recognized their marriage as lawful. Spyer died in 2009, leaving her estate to Windsor. If Windsor and Spyer’s union had been between opposite-sex spouses, Windsor would have qualified for the marital deduction and would therefore owe no federal estate tax. But because Windsor and Spyer were same-sex spouses, Windsor incurred a tax bill in excess of \$360,000.

Windsor sued for a refund. DOMA's exclusion of same-sex couples lawfully married under state law from the federal definition of marriage, she contended, violated the equal protection component of the Fifth Amendment. The District Court granted summary judgment in favor of Windsor, held DOMA's §3 unconstitutional, and awarded the refund Windsor sought. The Court of Appeals affirmed and the Supreme Court granted the government's petition for review.

But by then, the government no longer defended the constitutionality of §3. So the Court faced a threshold question: Did the executive branch's agreement with the decisions of the District Court and Second Circuit deprive the Supreme Court of jurisdiction?

In an opinion by Justice Kennedy, joined by Justices Breyer, Sotomayor, Kagan, and me, the Court first determined that Windsor's case remained a live controversy notwithstanding the government's agreement with her that §3 of DOMA was unconstitutional. The government had not refunded the estate tax Windsor paid, and the order requiring it to do so, the Court held, sufficed to render the government an aggrieved party with standing to invoke the Court's jurisdiction.

On the merits, the Court held that DOMA's §3 could not withstand measurement against the Constitution's guarantees of equal protection and due process. In design and effect, Justice Kennedy wrote, §3 treated state-sanctioned same-sex marriages "as second-class marriages for [federal law] purposes." Or, as I remarked at oral argument, DOMA rendered them skim-milk marriages. Our constitutional commitment to equality, Justice Kennedy stated, "'must at the very least mean that a bare congressional desire to harm a politically unpopular group'" does not justify disadvantageous treatment. The opinion also sounds a federalism theme: regulation of domestic relations traditionally has been left largely to state governance. Federal displacement of state law in that domain, the Court said, bears close review.

Dissenting opinions were filed by the Chief Justice, Justice Alito, and Justice Scalia, joined by Justice Thomas. Justice Scalia summarized his spirited dissent from the bench. Regarding standing, he urged that the Court's "authority [under Article III] begins and ends with the need to adjudge the rights of an injured party." Once the government agreed with Windsor's position, he maintained, it was inevitable that her injury would be redressed. On the merits, Justice Scalia said, §3 of DOMA had several legitimate aims, among them, §3 provided a stable, uniform definition of marriage for the many federal statutes in which marriage matters.

From the current term, a most significant case, in addition to the contraceptive coverage and recess appointment cases, is *McCutcheon v. Federal Election Commission*. The plaintiffs in that case challenged the aggregate spending limits set by the Bipartisan Campaign Reform Act of 2002. The Act imposed two types of limits on campaign contributions: "base" limits, restricting the total amount of money a donor may contribute to an individual candidate or committee, and "aggregate" limits, restricting the total amount of money a donor may contribute to all candidates and committees in an election. The plaintiffs—the Republican National Committee and a high-dollar political donor named Shaun McCutcheon—argued that the aggregate limits impermissibly restrained political speech in violation of the First Amendment.

A three-judge District Court in the District of Columbia dismissed the suit as foreclosed by the Supreme Court's pathmarking 1976 decision in *Buckley v. Valeo*. *Buckley* upheld the then-applicable base and aggregate limits. Base limits, the Court explained in *Buckley*, served to prevent "the actuality and appearance of corruption resulting from large individual financial contributions," and aggregate limits "serve[d] to prevent evasion" of the base limits. Without an aggregate limit, *Buckley* observed, a donor could "contribute massive amounts of money to a particular candidate through the use of unearmarked contributions to political committees likely to contribute to that candidate," thereby rendering base limits an exercise in futility. The three-judge District Court panel in *McCutcheon* found dispositive *Buckley*'s holding that aggregate limits encounter no First Amendment shoal.

In a 5 to 4 decision, the Supreme Court reversed, invalidating aggregate limits. The Chief Justice, in a plurality opinion joined by Justices Kennedy, Scalia, and Alito, wrote that *Buckley* did not control because the "statutory safeguards against circumvention have been considerably strengthened since *Buckley* was decided." Under the current statutory regime, the plurality concluded, the base limits suffice to prevent "quid pro quo" corruption. Discounted by the plurality was the interest, advanced by the Solicitor General, in preventing individuals from spending large sums of money to obtain ready access to, and influence over, elected officials. Justice Thomas supplied the fifth vote to invalidate aggregate limits. He would have overruled *Buckley v. Valeo* in its entirety.

Justice Breyer's dissent, joined by Justice Sotomayor, Justice Kagan, and me, deplored the Court's narrowing of "corruption" to the quid pro quo kind. Congress, whose members know better than the Court what money can buy, Justice Breyer reasoned, targeted "'the broader threat from politicians too compliant with the wishes of large contributors.' "

The dissent also took issue with the Court's assertion that amendments to campaign finance legislation rendered aggregate limits obsolete. Absent aggregate limits, Justice Breyer spelled out, numerous mechanisms would enable donors to "channel millions of dollars to parties and to individual candidates," yielding the very "kind of 'corruption' or 'appearance of corruption' that previously led the Court to [up]hold aggregate limits."

Affirmative action returned to the Court this term in *Schuette v. Coalition to Defend Affirmative Action*, a case we took up from the Sixth Circuit. In *Grutter v. Bollinger*, decided in 2003, the Court had upheld the University of Michigan Law School's affirmative action plan. Thereafter, by ballot initiative, Michigan voters approved an amendment to the State's Constitution banning resort to affirmative action measures by public institutions. Proponents of affirmative action, including students and faculty at Michigan's public universities, challenged the amendment to Michigan's Constitution as incompatible with the Equal Protection Clause.

A sharply divided Sixth Circuit, sitting en banc, reversed the District Court's decision, which had upheld the affirmative action ban. The ballot initiative, the Sixth Circuit majority held, was at odds with Supreme Court decisions in two cases: *Hunter v. Erickson*, in 1969, and *Washington v. Seattle School District Number 1*, in 1982. Both decisions held it unconstitutional to "remov[e] the authority to address a racial problem—and only a racial problem—from [an] existing decisionmaking body, in such a way as to burden minority interests." The amendment to

Michigan's Constitution did just that, the Sixth Circuit concluded, for it removed power over race-conscious admissions policies from the governing bodies of Michigan's public universities, which had controlled such policies in the past.

A splintered Supreme Court reversed the Sixth Circuit's judgment. Justice Kennedy, joined by the Chief Justice and Justice Alito, authored the lead opinion. In their view, *Hunter* and *Seattle* did not govern, for the laws challenged in those cases "aggravat[ed] . . . [a pre-existing] racial injury." Concurring in the judgment only, Justice Breyer agreed that *Seattle* and *Hunter* were distinguishable. No preexisting political process was affected by the amendment, Justice Breyer said, because unelected faculty members, not any elected decisionmakers, had previously determined admissions policies at Michigan's schools. Justice Scalia, joined by Justice Thomas, also concurred in the judgment. *Hunter* and *Seattle* were on point, they thought, but those decisions, Justice Scalia said, were undermined by later rulings and should be overruled.

Justice Sotomayor dissented in an impassioned opinion I joined. By constitutionalizing the question of race-conscious admissions, the Michigan amendment, like the laws held invalid in *Hunter* and *Seattle*, Justice Sotomayor wrote, "stymie[d] the right of racial minorities to participate in the political process." Disagreeing with the view that courts should "leave race out of the picture entirely and let the voters [decide]," Justice Sotomayor described the many ways in which race still matters in our society, ways she ranked impossible to ignore.

Back to Second Circuit cases, the Court decided *Town of Greece v. Galloway*, 5 to 4. Greece, a town near Rochester with a population of 94,000, has, since 1999, invited clergy members to perform prayers at monthly meetings of its Town Board. From the inception of the practice until the Town received complaints, all the participating ministers were Christian, and about two-thirds of the prayers referred to "Jesus," "Christ," "the Holy Spirit," or made similar sectarian invocations.

The plaintiffs, Susan Galloway and Linda Stephens, were non-Christians who lived in Greece and attended Town Board meetings to speak on issues of local concern. The opening prayers, they argued, violated the First Amendment's Establishment Clause.

The District Court upheld the Town's prayer practice, relying on the Supreme Court's decision in *Marsh v. Chambers*, which rejected an Establishment Clause challenge to daily opening prayers in Nebraska's legislature. The *Marsh* Court cautioned, however, that the prayers offered must not "proselytize or advance any one, or . . . disparage any other, faith or belief." The Second Circuit reversed the District Court's decision. Aspects of the prayer program, the court concluded, conveyed the message that Greece was endorsing Christianity.

The Supreme Court reversed the Second Circuit's judgment, 5 to 4. Greece's prayer practice, Justice Kennedy wrote for the majority, was not significantly different from the practice of the Nebraska legislature upheld in *Marsh*.

Justice Kagan dissented, joined by Justice Breyer, Justice Sotomayor, and me. Greece's practice differed from the practice *Marsh* upheld, Justice Kagan reasoned, because prayers at Greece's Town Board meetings were directed not to Town Board members in particular, but to all Town residents in attendance. "[M]onth in and month out, for over a decade," Justice

Kagan wrote, “prayers steeped in only one faith [and] addressed toward members of the public [had] commenced meetings to discuss local affairs and distribute government benefits.” This practice, she concluded, “d[id] not square with the First Amendment’s promise that every citizen, irrespective of her religion, owns an equal share in her government.” No citizen, the dissent urged, should be made to feel herself an outsider.

Last on my list for this morning, a Second Circuit case still awaiting decision, ABC v. Aereo. Respondent Aereo allows its subscribers, in exchange for a monthly fee, to “Watch Live TV Online.” To provide this service, Aereo employs thousands of dime-sized antennas. When a user opts to watch or record a program, an antenna is assigned exclusively, but temporarily, to the user and tuned to the desired channel. Aereo then saves that program in a user-specific directory. Why the thousands of individualized antennas and copies? Aereo relied on a 2008 Second Circuit decision in a case known as *Cablevision*. The court in *Cablevision* held that, under the transmit clause of the Copyright Act, no public performance is involved when a cable operator remotely records and stores particular programs for later viewing on demand by individual subscribers.

Aereo advertises its service as an innovative and convenient means for users to watch and record broadcast television. Others see Aereo as a business that free rides on copyrighted works, thereby obtaining an unfair competitive advantage over copyright licensees. Dissenting from the Second Circuit opinion now under review, Judge Chin called Aereo’s scheme “a Rube Goldberg-like contrivance, over-engineered in an attempt to avoid the reach of the Copyright Act.” Late in June, you will know which view prevails.

## **Appendix C: Excerpts from *Scalia/Ginsburg***

An American opera in one act by DERRICK WANG  
Libretto by the composer

Inspired by the opinions of U.S. Supreme Court Justices  
RUTH BADER GINSBERG and ANTONIN SCALIA  
and operas by HÄNDEL, MOZART, VERDI BIZET, et al.

*Justice will be sung.*

### **Aria: “The Justices are blind!” (Scalia)**

#### **SCALIA:**

This court’s so changeable—  
As if it’s never, ever known the law!

The Justices are blind!  
How can they possibly spout this—?  
The Constitution says absolutely nothing about this,  
This right that they’ve enshrined—  
When did the document sprout this?  
The Framers wrote and signed  
Words that endured without this;  
The Constitution says absolutely nothing about this!  
  
We all know well what the Framers did say,  
And (with certain amendments) their wording will stay,  
And these words of our Fathers limit us,  
For we are unelected,  
And thus, when we interpret them,  
Rigor is expected.

#### **SCALIA (cont’d):**

Oh, Ruth, can you read? You’re aware of the text,  
Yet so proudly you’ve failed to derive its true meaning,  
And never were so few  
Rights made so numerous—  
It’s almost humorous  
What you construe!  
Oh, well; oh, well; oh, well; oh, well;  
You are the reason I have to rebel!

Though you are all aligned  
In your decision to flout this,  
The Constitution says absolutely nothing about this—  
So, though you have combined,  
You would do well not to doubt this:  
Since I have not resigned,  
I will proceed to shout this:  
“The Constitution says absolutely nothing about this!”

Copyright © 2012–2015 Derrick Wang. All rights reserved. Possession of this publication does not constitute a license to reprint or perform this material. For inquiries regarding the publishing, licensing, and/or performance of material from *Scalia/Ginsburg*, please contact [info@derrickwang.com](mailto:info@derrickwang.com).

### Aria & Variations: “You are searching in vain (for a bright-line solution)” (Ginsburg)

#### GINSBURG:

How many times must I tell you,  
Dear Mister Justice Scalia:  
You'd spare us such pain  
If you'd just entertain  
This idea...  
(Then you *might* relax your rigid posture.)

*(À la Verdi)*

You are searching in vain for a bright-line solution  
To a problem that isn't so easy to solve—  
But the beautiful thing about our Constitution  
Is that, like our society, it can evolve.

For the Founders, of course, were great men with a vision,  
But their culture restricted how far they could go,  
So, to us, I believe, they bequeath the decision  
To allow certain meanings to flourish and grow.  
Let 'em grow...

*(Jazz waltz)*

For the law of the land in that era was grounded  
In the notion that justice was just for the few,  
But the Founders' assumption was wholly unfounded,  
So we've had to subject it to further review.

#### GINSBURG (cont'd):

So we're freeing the people we used to hold captive,  
Who deserve to be more than just servants or wives.  
If we hadn't been willing to be so adaptive,  
Can you honestly say we'd have led better lives?

*(Gospel-pop ballad)*

And we can't wait for slow legislation  
To catch up with the lives that we already lead;  
We have rights, and they need preservation,  
And we have to remember this if we intend to succeed:

Though we won't be afraid of forgiving,  
We must not stop in our mission to right every wrong—  
Not until We the People and our Constitution are living  
In a nation, in a place  
That, regardless of station or race,  
Is a nation where *all* of us truly belong!

*(À la Verdi)*

So, until every person is treated as equal  
Well beyond what the Founders initially saw,  
Let our past and our present be merely the prequel  
To a future enlightened by flexible law!

*(Roulades in all three styles: opera, jazz, and pop)*  
Law, law, law!

### Duet: “We are different. We are one” (Scalia, Ginsburg)

#### SCALIA, GINSBURG:

Yes:

We are different.  
We are one.  
The U.S. contradiction—

#### SCALIA:

The tension we adore:

**SCALIA, GINSBURG:**  
Sep'rate strands unite in friction  
To protect our country's core.  
This, the strength of our nation,  
Thus is our Court's design:  
We are kindred,  
We are nine.

#### SCALIA:

To strive for definition,

#### GINSBURG:

To question and engage,

#### SCALIA:

Let us speak to our tradition—

#### GINSBURG:

Or address a future age.

#### SCALIA:

This, the duty upon us...

#### GINSBURG:

This, the freedom...

#### SCALIA, GINSBURG:

...To judge how our strands are spun:  
This makes us different:

#### SCALIA:

We are one...

#### GINSBURG:

We are one decision from forging the source of  
tomorrow...

#### SCALIA:

One decision from shifting the tide...

#### SCALIA, GINSBURG:

Always one decision from charting the course we will  
steer...  
For our future  
Is unclear,  
But one thing is constant—  
The Constitution we revere.

We are stewards of this trust;  
We uphold it as we must,  
For the work of our Court is just  
Begun...

And this is why we will see justice done:  
We are different;  
We are one.

## **Appendix D: *In Memoriam***

The 2014 Judicial Conference honored the memory of five judges who passed away since the 2012 Judicial Conference:

- 1) Honorable Joseph M. McLaughlin, Senior United States Circuit Judge, Court of Appeals for the Second Circuit;
- 2) Honorable Mark R. Kravitz, United States District Judge, District of Connecticut;
- 3) Honorable Peter K. Leisure, Senior United States District Judge, Southern District of New York;
- 4) Honorable Harold Baer Jr., Senior United States District Judge, Southern District of New York; and
- 5) Honorable Burton R. Lifland, United States Bankruptcy Judge, Southern District of New York.

## **Appendix E: Introduction of New Judges**

The 2014 Judicial Conference welcomed twenty new judges who joined the Circuit since the 2012 Judicial Conference:

1. Honorable Mark A. Barnett, United States Court of International Trade

Mark A. Barnett was previously an attorney in the international trade group at Steptoe & Johnson. He left the firm to join the Office of Chief Counsel for Import Administration at the U.S. Department of Commerce, where he served as a staff attorney, a senior counsel and subsequently the Deputy Chief Counsel for Import Administration. In 2008-2009, Judge Barnett was detailed to the U.S. House of Representatives, Committee on Ways and Means, and Subcommittee on Trade as a Trade Counsel.

Judge Barnett graduated from Dickinson College in 1985 and received his law degree from the University of Michigan Law School in 1988.

2. Honorable Vernon S. Broderick, United States District Judge, Southern District of New York

Prior to his appointment to the bench in 2013, Vernon S. Broderick was a partner at Weil, Gotshal & Manges, LLP focusing on white collar criminal cases, regulatory investigations and business litigation. From 1994 until 2002, he served as an Assistant United States Attorney in the Southern District of New York.

Judge Broderick graduated from Yale University in 1985 and received his law degree from Harvard Law School in 1988.

3. Honorable Valerie E. Caproni, United States District Judge, Southern District of New York

Valerie E. Caproni was Deputy General Counsel of Northrop Grumman Corp. until becoming a U.S. District Judge in 2014. She was General Counsel of the FBI from 2003 until 2011. She previously worked as an Assistant United States Attorney in the Eastern District of New York and as Regional Director of the Pacific Regional Office of the Securities and Exchange Commission in Los Angeles.

Judge Caproni graduated from Tulane University in 1976 and received her law degree from the University of Georgia School of Law in 1979.

4. Honorable Pamela Ki Mai Chen, United States District Judge, Eastern District of New York

Pamela Ki Mai Chen was an Assistant U.S. Attorney in the Eastern District of New York for almost 15 years before becoming a U.S. District Judge in 2013. She was Chief of the Civil Rights Section, Deputy Chief of the Public Integrity Section and Chief of Civil Rights Litigation. She previously served as a Senior Trial Attorney in the Civil Rights Division of the U.S. Department of Justice.

Judge Chen graduated from the University of Michigan in 1983 and received her law degree from the Georgetown University Law Center in 1986.

5. Honorable Katherine Polk Failla, United States District Judge, Southern District of New York

From 2000 until becoming a U.S. District Judge in 2013, Katherine Polk Failla was an Assistant United States Attorney in the Southern District of New York. In 2008, she became Chief of the Criminal Appeals Unit. She previously worked as an associate in the Securities Litigation and Enforcement practice group of Morgan, Lewis & Bockius LLP.

Judge Failla graduated from the College of William & Mary in 1990 and received her law degree from Harvard Law School in 1993.

6. Honorable Frank P. Geraci, Jr., United States District Judge, Western District of New York

Frank Paul Geraci, Jr. was a Monroe County Court Judge from 1999 until 2013, when he was appointed as a U.S. District Judge. Before becoming a judge, he practiced civil and criminal litigation at a firm he founded, Geraci and Feldman. He also served as an Assistant District Attorney and as an Assistant United States Attorney in the Western District of New York.

Judge Geraci graduated from the University of Dayton in 1973 and received his law degree from the University of Dayton Law School in 1977.

7. Honorable Christian F. Hummel, United States Magistrate Judge, Northern District of New York

Prior to his appointment in 2012, Christian F. Hummel held various judicial positions in state and local government: Rensselaer County Surrogate (2002-2012); Rensselaer County Family Court Judge (1993-2002); and Town Justice in the town of East Greenbush (1986-1993). He previously was a partner at the New York law firm of Carter & Conboy, where his practice centered on civil litigation and trial work.

Judge Hummel graduated from the University of New York at Plattsburgh in 1977 and received his law degree from Albany Law School in 1981.

8. Honorable Claire R. Kelly, United States Court of International Trade

Prior to her appointment to the bench, Claire R. Kelly was a tenured faculty member of Brooklyn Law School where she taught for 15 years. While at Brooklyn Law School, Judge Kelly focused her scholarship on Administrative Law and International Trade Law.

Judge Kelly graduated from Barnard College in 1987 and received her law degree from Brooklyn Law School in 1993.

9. Honorable Louis A. Scarella, United States Bankruptcy Court, Eastern District of New York

Louis A. Scarella began his legal career with the law firm of Phillips, Nizer, Benjamin, Krim & Ballon in 1977, becoming a partner in 1983. From 2005 until he was appointed to the bench, Judge Scarella was a shareholder with the law firm Farrell Fritz, P.C.

Judge Scarella graduated from Providence College in 1973 and received his law degree from Hofstra Law School (now known as The Maurice A. Deane School of Law at Hofstra University) in 1977.

10. Honorable Lorna G. Schofield, United States District Court, Southern District of New York

Lorna G. Schofield was a litigation partner at the law firm of Debevoise & Plimpton LLP from 1991 to 2011. Judge Schofield's practice focused on litigation in complex commercial matters. From 1984 to 1988, Judge Schofield served as an Assistant U.S. Attorney in the Southern District of New York.

Judge Schofield graduated from Indiana University in 1977 and received her law degree from New York University School of Law in 1981.

11. Honorable Michael P. Shea, United States District Court, District of Connecticut

Michael P. Shea was previously a partner with Day, Berry & Howard LLP, where he focused on commercial litigation, mass torts, First Amendment matters and white collar criminal defense. He also chaired the firm's appellate practice group.

Judge Shea graduated from Amherst College in 1989 and received his law degree from Yale Law School in 1993.

12. Honorable Analisa Torres, United States District Court, Southern District of New York

Analisa Torres served on the New York State bench from 2000-2013 in the Supreme, Criminal and Civil Courts. Prior to that, she was a law clerk for a New York State Supreme Court Justice and an associate at several law firms.

Judge Torres graduated from Harvard College in 1981 and received her law degree from Columbia Law School in 1984.

13. Honorable Elizabeth A. Wolford, United States District Court, Western District of New York

Before assuming the bench, Elizabeth A. Wolford practiced for over twenty years with The Wolford Law Firm LLP, where she concentrated in commercial and employment litigation.

Judge Wolford graduated from Colgate University in 1989 and received her law degree from Notre Dame Law School in 1992.

14. Honorable Gregory H. Woods, United States District Court, Southern District of New York

From 1995 until 1998, Gregory H. Woods was a Trial Attorney in the Civil Division of the United States Department of Justice in Washington, D.C. Judge Woods joined Debevoise & Plimpton in 1998 and became a partner in 2004. In 2009, Judge Woods left Debevoise to serve as Deputy General Counsel of the United States Department of Transportation and later served as General Counsel of the United States Department of Energy.

Judge Woods graduated from Williams College in 1991 and received his law degree from Yale Law School in 1995.

15. Honorable Julie A. Manning, United States Bankruptcy Judge, District of Connecticut

Julie A. Manning was in private practice for twenty-five years prior to her appointment, representing a variety of clients in bankruptcy cases throughout the United States. From 1999 until her appointment in 2013, Judge Manning was a partner with Shipman & Goodwin, LLP.

Judge Manning graduated from Fairfield University in 1983 and received her law degree from Suffolk University in 1988.

16. Honorable Judith McCarthy, United States Magistrate Judge, Southern District of New York

From 1992 to 1998, Judith McCarthy served in the New York City Corporation Counsel's Office, ultimately serving as a Deputy Assistant Chief in the General Litigation Division. From 1998 to 2002, Judge McCarthy served at the New York City Human Resources Administration, rising to be First Deputy General Counsel. Judge McCarthy then joined the New York State Attorney General's Office, where she was named Assistant Attorney General-in-Charge of the Westchester Regional Office. In January 2011, Judge McCarthy was Executive Vice President and General Counsel of the New York Power Authority.

Judge McCarthy graduated from Barnard College in 1987 and received her law degree from CUNY Law School in 1991.

17. Honorable Jeffrey Alker Meyer, United States District Judge, District of Connecticut

Jeffrey A. Meyer began his practice career in 1992 as a staff attorney with Vermont Legal Aid and later as a corporate litigator from 1993 to 1995 in Washington, D.C. From 1995 to 2004, Judge Meyer served as an Assistant United States Attorney in the District of Connecticut. From 2004 to 2005, he served in New York as Senior Counsel to the Independent Inquiry into the United Nations Oil-for-Food Program in Iraq. From 2006 to 2014, Judge Meyer was a professor at Quinnipiac University School of Law, and from 2010 to 2014, he also served as a visiting professor at Yale Law School.

Judge Meyer graduated from Yale College in 1985 and received his law degree from Yale Law School in 1989.

18. Honorable Sarah Netburn, United States Magistrate Judge, Southern District of New York

Prior to her appointment, Sarah Netburn was a partner at Emery Celli Brinckerhoff & Abady LLP in New York. She served as Chief Counsel to the Office of Pro Se Litigation for the United States District Court for the Southern District of New York from 2010 to 2012.

Judge Netburn graduated from Brown University in 1994 and received her law degree from the University of California at Los Angeles School of Law in 2001.

19. Honorable Nelson Stephen Román, United States District Judge, Southern District of New York

Nelson S. Román was an Associate Justice of the First Appellate Division of the New York State Supreme Court from 2009 to 2013. He also served as a Justice of the New York Supreme Court in Bronx County from 2003 to 2009, and as a Judge of the New York City Civil Court from 1998 to 2002. Before becoming a judge, Judge Román served as an Assistant District Attorney in Brooklyn and Manhattan.

Judge Román graduated from Fordham University in 1984 and received his law degree from Brooklyn Law School in 1989.

20. Honorable Vera M. Scanlon, United States Magistrate Judge, Eastern District of New York

Vera M. Scanlon began her legal career as an associate with the law firm of Hughes Hubbard & Reed LLP. From 2001 to 2012, Judge Scanlon worked as a litigator with Beldock Levine & Hoffman LLP, where she primarily litigated civil rights and commercial cases.

Judge Scanlon graduated from Columbia College in 1990 and received her law degree from Yale Law School in 1995.





## **Members of the Program and Planning Committee**

Hon. Robert A. Katzmann, Chief Judge

Hon. Victor Marrero, Chairman

Ms. Karen Greve Milton, Circuit Executive

Honorable Janet Bond Arterton

Thomas A. Brown, Esq.

Honorable Andrew T. Baxter

Evan Chesler, Esq.

Honorable Margaret Cangilos-Ruiz

David Cleary, Esq.

Honorable Shelley Chapman

John Cronan, Esq.

Honorable Brian Cogan

Dean Matthew Diller

Honorable John M. Conroy

Raymond Dowd, Esq.

Honorable Paul Crotty

James I. Glasser, Esq.

Honorable Mae D'Agostino

Ken Hashimoto, Esq.

Honorable Paul Engelmayer

Carol E. Heckman, Esq.

Honorable Kevin Fox

Ellen V. Holloman, Esq.

Honorable Marilyn Go

Robert D. Maldonado, Esq.

Honorable John G. Koeltl

Dean Michael M. Martin

Honorable William Kuntz

Charles Michael, Esq.

Honorable Roslynn Mauskopf

Kelly A. Moore, Esq.

Honorable Andrew J. Peck

Professor Samuel Rascoff

Honorable Cathy Seibel

Harry H. Rimm, Esq.

David Anders, Esq.

Jacqueline Silberman, Esq.

Robert Anello, Esq.

Michael Tremonte, Esq.

James Benjamin, Esq.

Alan Vinegrad, Esq.

Michael Bosworth, Esq.

