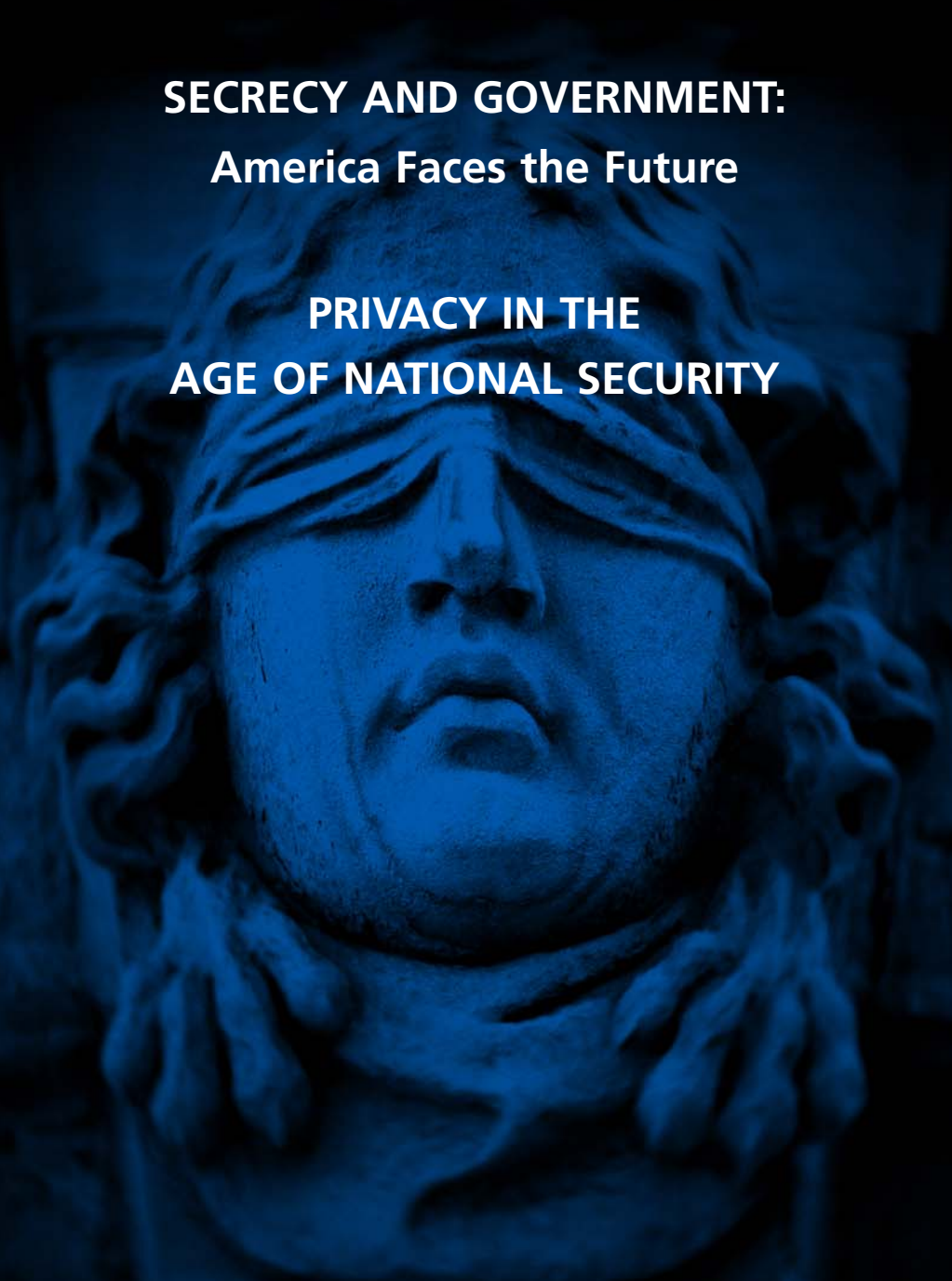




THE CENTER ON LAW AND SECURITY AT THE NYU SCHOOL OF LAW

**SECRECY AND GOVERNMENT:
America Faces the Future**

**PRIVACY IN THE
AGE OF NATIONAL SECURITY**





THE CENTER ON LAW AND SECURITY AT THE NYU SCHOOL OF LAW

SECRECY AND GOVERNMENT: America Faces the Future

PRIVACY IN THE AGE OF NATIONAL SECURITY

Editor in Chief: Karen J. Greenberg

Editor: Jeff Grossman

Copy Editor: Sybil Perez

Research: Joe Ortega, Summer Walker

Index: Jim Diggins

Design: Wendy Bedenbaugh

copyright © 2009 by the Center on Law and Security
cover photo: [photo@istockphoto.com/Duncan Walker](http://photo@istockphoto.com/Duncan_Walker)

The opinions of the speakers herein do not represent the opinions of the Center on Law and Security.



The dual concepts of secrecy and privacy were the subject of much scrutiny under the Bush administration. In two separate conferences held in 2007 at the Center on Law and Security, participants discussed the administration's stance regarding these intertwined ideas. As Barton Gellman described, "national security presents a conflict of core values in our society between self-government and self-defense." Covering a broad spectrum of issues and perspectives, the conversations at the conferences highlighted questions about the nature of power in the context of national security, the consequences of government secrecy, and invasions into the private realm of U.S. citizens.

At both events, panelists set out the facts of what occurred in the name of national security during the war on terror. In the matter of secrecy, government officials expanded their right to keep information out of the public eye, thereby increasing their authority. "When we allow information to concentrate or to accumulate in the executive branch, or anywhere," Jameel Jaffer said, "we are allowing power to concentrate there as well." The number of classified documents grew exponentially. Relying upon the states secrets privilege, the government persuaded courts to dismiss cases in which individuals claim to have been tortured – in the case of Khaled el-Masri, apparently due to mistaken identity. The torture policy and the CIA ghost prisons were kept secret not only from the public but also from many officials in Washington.

In the matter of privacy, our panelists told us the reverse circumstance occurred. While secrecy mounted, privacy was eroded. The customary government respect for the privacy of its citizens diminished notably, according to our experts who cited the use of national security letters to collect information about individuals on an exponentially greater scale. We also discovered that our ability to retain our privacy amidst rapid technological expansion has been reduced to nearly nil, and that a thriving commerce exists relative to personal information.

In some areas, discussion turned to the places where privacy and secrecy overlap, thus highlighting their mirror relationship to one another. This was particularly apparent in the matter of warrantless wiretapping. Although we still, in the early months of the Obama administration, do not know the full extent of the covert warrantless wiretapping program, the government appears to have monitored a number of citizens' conversations in defiance of previously accepted legal, not to mention ethical, standards.

In some instances, the analyses of the individual right to privacy and the governmental right to secrecy varied considerably. As Jeff Jonas noted in regard to the commercial use of personal information, but which is equally true of the broader discussion, "the policy debate comes down to who gets to peek at the data, when, and with what oversight and accountability?"

Yet the overall consensus of participants at both conferences was that government augments its power by keeping information secret, even between various government agencies. At the same time, individuals and society collectively lose a cherished right when privacy is removed or even compromised. As Professor Burt Neuborne said, "the feeling that we are being watched, whether or not we actually are, creates a deterrence on non-conventional behavior for which our culture will eventually pay a price." Today, the ideas at the heart of these two conferences remain vital and instructive about the questions underlying the way forward as the country accepts the mission of protecting both civil liberties and national security.

A handwritten signature in black ink, reading "Karen J. Greenberg". The signature is fluid and cursive, with the first name being the most prominent.

Karen J. Greenberg, Executive Director

Table of Contents

SECURITY AND GOVERNMENT: America Faces the Future

Participant Biographies	8
On Secrets and Secrecy	14
Gaining Perspective: Secrecy Then and Now	18
Panelists: Scott Horton, Col. W. Patrick Lang, Walter Pincus, Michael Sheehan Moderator: Prof. Noah Feldman	
Secrecy and Decision-Making	30
Panelists: Barton Gellman, Prof. Jack Goldsmith, Prof. Stephen Holmes Moderator: Prof. Richard Pildes	
The War on Terror and the Courts	44
Panelists: Elaine Cassel, Joshua Dratel, Anthony Lewis, Adam Liptak Moderator: Prof. Burt Neuborne	
National Security and Intelligence	58
Panelists: Frank Anderson, Jameel Jaffer, Judge Kenneth Karas,* Prof. Stephen Schulhofer Moderator: Dana Priest	
Afterword by Prof. Norman Dorsen	65

PRIVACY IN THE AGE OF NATIONAL SECURITY

Participant Biographies	70
Privacy: Then and Now	74
Panelists: Valerie Caproni, Robert O’Harrow, Jr., Prof. Geoffrey Stone Moderator: Prof. Burt Neuborne	
Citizens Surveilled: FISA, the Patriot Act and Today’s Telecommunications	88
Panelists: Bryan Cunningham, Barton Gellman, Prof. Stephen Schulhofer Moderator: Prof. Matthew Waxman	
Reins of Power: From Wall Street to Washington, D.C. and the Global Information Network	100
Panelists: Jeff Jonas, Vivian Maese, Declan McCullagh Moderator: Karen J. Greenberg	
Public, Private and Political Dangers	110
Panelists: Prof. Todd Gitlin, Lawrence Wright Moderator: Prof. Stephen Holmes	
Index	119
About the Center on Law and Security	126

*Judge Karas’s remarks were off the record.

A grayscale, heavily blurred image of a man's face, likely a historical figure, with a white cloth blindfolded over his eyes. The image is centered and serves as the background for the text.

**SECRECY AND GOVERNMENT:
America Faces the Future**

APRIL 12, 2007

Secrecy and Government: Participant Biographies; April 12, 2007

Frank Anderson has been a consultant on Middle East affairs to American and international businesses and to the U.S. and foreign governments since 1995. This follows a 27-year career in CIA, where his last assignment was as Chief of the Near East and South Asia Division. His other assignments included service as director of technical services, chief of the Afghan Task Force and 13 years in the field, where he served as the CIA's chief of station in three Middle Eastern countries.

Elaine Cassel practices law in Virginia and the District of Columbia, where she also teaches law and psychology. She is the author of a college textbook on criminal psychology. Her book *The War on Civil Liberties*, published in 2003, is an account of the early days of the Bush administration's "war on terror" and its impact on American citizens and the courts. Since 9/11, she has written and spoken about prosecution of terrorism cases in the Eastern District of Virginia and the Fourth Circuit Court of Appeals. She has appeared in several documentaries, is a commentator on radio programs in the U.S. and abroad, and has published articles in several foreign newspapers, including publications in Poland and Finland. She is a regular guest columnist for FindLaw's *Writ*.

Joshua L. Dratel is an attorney in New York City. Dratel, a past president of the New York State Association of Criminal Defense Lawyers and member of the Board of Directors of the National Association of Criminal Defense Lawyers, has been defense counsel in several terrorism and national security prosecutions, including those of Sami Omar Al-Hussayen, who was acquitted in federal court in Idaho in 2004, and Wadiah El-Hage, a defendant in *United States v. Usama bin Laden*, which

involved the August 1998 bombings of the United States embassies in Kenya and Tanzania. He was also lead and civilian counsel for David Hicks, an Australian detained at Guantanamo Bay, Cuba, in Mr. Hicks's prosecution by U.S. military commission, and currently represents Mohamed El-Mezain, a defendant in the federal prosecution of the Holy Land Foundation for Relief and Development, and, on appeal, Lynne Stewart, a New York lawyer convicted of material support for terrorism. He is co-editor with Karen J. Greenberg of *The Torture Papers: The Road to Abu Ghraib* (Cambridge University Press, 2005), a compendium of government memoranda.

Noah Feldman is the Cecilia Goetz Professor of Law at the New York University School of Law and an adjunct senior fellow at the Council on Foreign Relations. He specializes in constitutional studies, with particular emphasis on the relationship between law and religion, constitutional design, and the history of legal theory. In 2003, he served as senior constitutional advisor to the Coalition Provisional Authority in Iraq and subsequently advised members of the Iraqi Governing Council on the drafting of the Transitional Administrative Law, or interim constitution. He is the author of three books: *Divided By God: America's Church-State Problem and What We Should Do About It* (Farrar, Straus and Giroux, 2005); *What We Owe Iraq: War and the Ethics of Nation Building* (Princeton University Press, 2004); and *After Jihad: America and the Struggle for Islamic Democracy* (Farrar, Straus and Giroux, 2003). Feldman litigates constitutional cases before the federal courts; lectures on law, religion, and the Middle East; and is a contributing writer for *The New York Times Magazine*.

Barton Gellman is a special projects reporter on the national staff of *The Washington Post*, following tours as diplomatic correspondent, Jerusalem bureau chief, Pentagon correspondent, and D.C. Superior Court reporter. He shared the Pulitzer Prize for national reporting in 2002 and has been a jury-nominated finalist (for individual and team entries) three times. His work has also been honored by the Overseas Press Club, the Society of Professional Journalists (Sigma Delta Chi), and the American Society of Newspaper Editors. He is author of *Contending with Kennan: Toward a Philosophy of American Power*, a study of the post-World War II “containment” doctrine and its architect, George F. Kennan.

Jack Goldsmith is Henry L. Shattuck Professor of Law at Harvard University, specializing in international law, foreign affairs law, conflicts of law, and national security law. He is the author of dozens of articles on these and other subjects. His most recent publications are *Who Controls the Internet? Illusions of a Borderless World* (Oxford Press 2006, with Tim Wu) and *The Limits of International Law* (Oxford Press 2005, with Eric Posner). Before coming to Harvard, he served as assistant attorney general, Office of Legal Counsel, from October 2003 through July 2004, and special counsel to the general counsel to the Department of Defense from September 2002 through June 2003. Professor Goldsmith taught at the University of Chicago Law School from 1997-2002, and at the University of Virginia Law School from 1994-1997.

Karen J. Greenberg is the executive director of the Center on Law and Security. She is the editor of the *NYU Review of Law and Security*, co-editor of *The Torture Papers: The Road to Abu Ghraib*, and editor of the books *Al Qaeda Now* and *The Torture Debate in America* (Cambridge University Press). She is a frequent writer and commentator on issues related to national secu-

rity, terrorism, and torture and has authored numerous articles on the United States and Europe during World War II. She is a former vice president of the Soros Foundation/Open Society Institute and the founding director of the Program in International Education. She is an editor of the Archives of the Holocaust, Columbia University Series, and has served as a consultant to the National Endowment for the Humanities, the NY Council for the Humanities, the NYC Board of Education, and USAID.

Stephen Holmes is a faculty co-director at the Center on Law and Security and the Walter E. Meyer Professor of Law at the NYU School of Law. His fields of specialization include the history of liberalism, the disappointments of democratization after communism, and the difficulty of combating terrorism within the limits of liberal constitutionalism. In 2003, he was selected as a Carnegie Scholar. He was a professor of politics at Princeton from 1997 to 2000, professor of politics and law at the law school and political science department of the University of Chicago from 1985 to 1997, and taught at Harvard University’s Department of Government from 1979 to 1985. He was the editor in chief of the *East European Constitutional Review* from 1993-2003. He is the author of *Benjamin Constant and the Making of Modern Liberalism* (Yale University Press, 1984), *The Anatomy of Antiliberalism* (Harvard University Press, 1993), *Passions and Constraint: On the Theory of Liberal Democracy* (University of Chicago Press, 1995), and co-author (with Cass Sunstein) of *The Cost of Rights: Why Liberty Depends on Taxes* (Norton, 1999). His newest book, *The Matador’s Cape: America’s Reckless Response to the War on Terror* was published in 2007.

Scott Horton is an attorney, commentator, and a lecturer at Columbia Law School. He is the author of over 100 articles and monographs on law reform in the former Soviet Union and other socialist and formerly socialist states, with an emphasis on the commercial sector as well as the law of armed conflict and human rights topics. He has also acted as an advisor on law reform issues to five governments in the Eurasian region. Horton is a member of the Council on Foreign Relations; chairs the advisory board of the EurasiaGroup, a think-tank working in the Eurasian region; and was the founding trustee of the American University in Central Asia, a higher education project launched by the U.S. and Kyrgyz governments and the Soros Foundation. He served as counsel to Andrei Sakharov and Elena Bonner, among other human rights advocates. He headed a series of inquiries on behalf of the organized bar into detainee abuse issues associated with the war on terror. He is a director of the International Law Association, chairs the New York City Bar Association's Committee on International Law, and previously chaired several other committees.

Jameel Jaffer is a litigator for the American Civil Liberties Union and deputy director of the ACLU's National Security Program. Currently, his docket includes *Doe v. Gonzales*, a challenge to the FBI's national security letter authority; *ACLU v. NSA*, a challenge to the constitutionality of warrantless surveillance conducted by the National Security Agency; *American Academy of Religion v. Chertoff*, a challenge to the government's refusal to grant a visa to Swiss scholar Tariq Ramadan; and *ACLU v. Department of Defense*, a litigation under the Freedom of Information Act for records concerning the treatment and detention of prisoners held by the U.S. in Afghanistan, Iraq, and at Guantanamo Bay. Prior to joining the staff of the ACLU, Jaffer served as law clerk to Hon. Amalya L. Kearse, United States Court

of Appeals for the Second Circuit, and then to Rt. Hon. Beverley McLachlin, chief justice of Canada.

Kenneth Karas is a United States district judge for the Southern District of New York. Upon graduating from law school, he served as a law clerk to the Hon. Reena Raggi, then United States district judge for the Eastern District of New York. Thereafter, he served as an assistant United States attorney for the Southern District of New York from 1992 until 2001, and chief of the Organized Crime and Terrorism Unit from 2001 until his departure from the office in June 2004. While at the U.S. Attorney's Office, Judge Karas worked on numerous terrorism investigations into associates of several terrorist groups, including al Qaeda, Hamas, Egyptian Islamic Jihad, and the IRA. He was part of the team of prosecutors who in 2001 convicted four of Usama bin Laden's followers for their role in the August 1998 bombings of the American embassies in Nairobi and Dar es Salaam. He also participated in the prosecution of Zacarias Moussaoui, who pled guilty to being part of several conspiracies involving the September 11th terrorist attacks.

Colonel W. Patrick Lang is a retired senior officer of U.S. Military Intelligence and U.S. Army Special Forces (Green Berets). He served in the Department of Defense as a serving officer and as a member of the Defense Senior Executive Service. He is a highly decorated veteran of several overseas conflicts, including the war in Vietnam. He was the first professor of the Arabic language at the United States Military Academy at West Point. In the Defense Intelligence Agency, he was the defense intelligence officer for the Middle East, South Asia and terrorism, and later the first director of the Defense HUMINT (human intelligence) Service. He was awarded the Presidential Rank of Distinguished Executive, the equivalent of a British knighthood. He is an analyst and con-

sultant for many television and radio broadcasts, among them the *The NewsHour with Jim Lehrer* on PBS.

Anthony Lewis was a columnist for *The New York Times* from 1969 until December 2001. He won a Pulitzer Prize for national reporting in 1955 for a series of articles on the dismissal of a Navy employee as a security risk. Lewis won a second Pulitzer for his coverage of the Supreme Court in 1963 and the Presidential Citizens Medal in 2001. He is the author of three books: *Gideon's Trumpet*, *Portrait of a Decade*, and *Make No Law: The Sullivan Case and the First Amendment*. He was lecturer at Harvard Law School for 15 years, teaching a course on the Constitution and the press. He has taught at a number of other universities, including the universities of California, Illinois, Oregon, and Arizona. Since 1983, he has held the James Madison Visiting Professorship at Columbia University.

Adam Liptak is the national legal correspondent at *The New York Times*. He practiced law at a large New York City law firm and in the legal department of The New York Times Company before joining the paper's news staff in 2002. He was a member of the reporting teams that examined the Jayson Blair and Judith Miller scandals. He has covered the Supreme Court nominations of John Roberts and Samuel Alito; the investigation into the disclosure of the identity of Valerie Wilson, an undercover CIA operative; judicial ethics; and various aspects of the criminal justice system. In addition to the *Times*, Liptak's work has appeared in *The New Yorker*, *Vanity Fair*, *Rolling Stone*, and several law reviews.

Burt Neuborne is the legal director of the Brennan Center for Justice at the NYU School of Law. The Brennan Center, established in 1994 by the law clerks to Justice William Brennan, Jr. to honor his monumental contribu-

tion to American law, seeks to link the academic resources of a great law school and the practical skills of the bar in an effort to develop pragmatic approaches to problems that have resisted conventional solutions. Neuborne was appointed NYU law school's first John Norton Pomeroy Professor of Law in 1991 and received the university-wide Distinguished Teacher Award in 1990. He has been one of the nation's foremost civil liberties lawyers for 30 years, serving as national legal director of the ACLU, special counsel to the NOW Legal Defense and Education Fund, and as a member of the New York City Human Rights Commission. He challenged the constitutionality of the Vietnam War, pioneered the flag burning cases, worked on the *Pentagon Papers* case, worked with Justice Ruth Bader Ginsburg when she headed the ACLU Women's Rights Project, and anchored the ACLU's legal program during the Reagan years. Among Neuborne's best-known scholarly works is the two-volume *Political and Civil Rights in the United States* (with Norman Dorsen, Sylvia Law, and Paul Bender).

Richard Pildes is a faculty co-director at the Center on Law and Security and the Sudler Family Professor of Constitutional Law at the NYU School of Law. He specializes in constitutional law and legal issues involving the structure of democratic processes. He is the co-author of *Between Civil Libertarianism and Executive Unilateralism: An Institutional Process Approach to Rights During Wartime* (with Samuel Issacharoff) and the casebook *The Law of Democracy* (with Samuel Issacharoff and Pamela Karlan), and the author of numerous articles in the *Harvard Law Review*, the *Yale Law Journal*, the *Stanford Law Review*, the *University of Chicago Law Review*, the *Columbia Law Review*, and other leading legal journals. He was a professor of law at the University of Michigan Law School from 1988-2000, and clerked for Judge Abner J. Mikva of the United States Court of Appeals for the

District of Columbia Circuit and Justice Thurgood Marshall of the United States Supreme Court.

Walter Pincus first joined *The Washington Post* in 1966. He served as the executive editor of *The New Republic* from 1972-1975, after which he returned to the *Post* to write for the paper's national staff. When he resumed writing for the newspaper, he was also permitted to work as a part-time consultant to NBC News and later CBS News, developing, writing or producing television segments for network evening news, magazine shows, and documentaries. He became a consultant to the Washington Post Co. in 1988, for which he has explored new ventures, coordinating and producing joint editorial projects in print, electronic journalism, and television. Pincus has won several prizes, including a Pulitzer in 2001 for National Reporting, shared with four other *Post* reporters, for stories about Osama bin Laden; the George Polk Award in 1977 for stories in *The Washington Post* exposing the neutron warhead; the 1961 Page One award for magazine reporting in *The Reporter*; and an Emmy for writing a one-hour program in the 1981 CBS News documentary series *Defense of the United States*. He served in the U.S. Army Counterintelligence Corps, stationed in Washington, from 1955-1957 and has taken two sabbaticals from journalism to direct investigations for the Senate Foreign Relations Committee under its then-chairman, Sen. J. William Fulbright.

Dana Priest covers the intelligence community for *The Washington Post*, where she has worked for 15 years. She was the paper's Pentagon correspondent for six years and then wrote exclusively about the military as an investigative reporter. She was one of the first reporters on the ground for the invasion of Panama (1989), reported from Iraq in late 1990 just before the war began, and covered the 1999 Kosovo war from air bases in Europe. Priest is the author of

The Mission: Waging War and Keeping Peace With America's Military (W.W. Norton & Co., 2003). In 2001, she was awarded a prestigious MacArthur Foundation Research and Writing grant. The same year, she won the Gerald R. Ford Prize for Distinguished Reporting on the National Defense for her series "The Proconsuls: A Four-Star Foreign Policy?" and the State Department's Excellence in Journalism Award for the same series. She was the guest speaker and host for a four-part speaking series on the U.S. military and foreign policy for the Secretary's Open Forum. She also was a guest scholar in the residence at the U.S. Institute of Peace.

Stephen Schulhofer is the Robert B. McKay Professor of Law at the NYU School of Law and one of the nation's most distinguished scholars of criminal justice. He has written more than 50 scholarly articles and six books. His most recent book, *The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11*, written for The Century Foundation's Project on Homeland Security, has attracted wise attention as a careful and balanced critique of domestic measures being implemented as part of the "war on terrorism." He has written on police interrogation, the self-incrimination clause, administrative searches, drug enforcement, indigent defense, sentencing reform, plea bargaining, capital punishment, battered spouse syndrome, and other criminal justice matters. His current projects include an investigation of the growing practice of trying juveniles in adult court and an analysis of recent developments in the Supreme Court's interpretation of core Fifth Amendment principles. Previously the Julius Kreeger Professor of Law and director of studies in criminal justice at the University of Chicago Law School, Schulhofer was also the Ferdinand Wakefield Hubbell Professor of Law at the University of Pennsylvania. He clerked for two years for U.S. Supreme Court Justice Hugo

Black. Before teaching, he also practiced law for three years with the firm Coudert Freres, in France.

Michael Sheehan is best known for his counterterrorism work at the local, national, and international levels. Prior to his position as deputy commissioner of counterterrorism at the NYPD, Sheehan was appointed by Kofi Annan as the United Nations assistant secretary general in the Department of Peacekeeping Operations, where he was responsible for oversight of military and police peacekeeping forces around the world. Commissioner Sheehan's counterterrorism record extends back to the 1990s, when, following the embassy bombings in East Africa, he became the Department of State's ambassador at large for counterterrorism. Upon retiring from the Army as a lieutenant colonel in 1997, Sheehan was appointed a deputy assistant secretary of state in the Bureau of International Organizations, where he focused on international policing in Bosnia and Kosovo. He has served under three national security advisors and two presidents (George H.W. Bush and Bill Clinton).

On Secrets and Secrecy

Karen J. Greenberg:

Perhaps we should have called today's conference *Knowledge and Power* instead of *Secrecy and Government*. The relationship between knowledge and power – what those in power know and do not know, and what those who put people in power know and do not know – has forever been the essential dynamic of how we think of ourselves as a society.

One person who understood how to use knowledge for both good and evil was a rather unknown figure in American history – George Creel. Creel not only stood on top of President Woodrow Wilson's efforts during World War One and afterwards to find renegades, communists, and other people who were dangerous to the government and to weed them out, but he then went on to work for President Franklin Roosevelt as the person who could best inform the president as to the pulse of the nation. In other words, what you know and how you use it can be very different. It can be used for good. It can be used for ill.

People often ask me why we always have so many journalists and writers involved in Center on Law and Security events. Why aren't we satisfied to rely upon practitioners and experts who come out of the academy? The answer is that a huge burden has always been put on the media to monitor, explain, and serve as watchdogs for the nation. And this has been particularly true in the last six years. We, as citizens, rely upon the media to tell us what we need to know. Often, the journalists can provide the additional detail, the missing truth, that distinguishes confusion from understanding. But,

more importantly, we can learn from their skills, from their curiosity, and from their attentiveness. Like journalists, we as citizens need to make it a primary responsibility to heed the questions and discomforts that color our impressions of the world around us. And although we love to criticize the media, the fact is that this is a civic responsibility and, as such, is not only theirs but ours as well.

The Center on Law and Security is having this conference on government and secrecy today so that you, as the people listening, can begin to get in touch with the questions that

might concern us all about the role of government in the war on terror. The people whom we have brought here today are here solely to help us understand what questions we should be paying attention to and what kinds of issues we might want to take it upon ourselves to know about so that we all can develop an

informed opinion about those who are in charge of the business of the country.

Having said that, there are some people who take this responsibility particularly seriously as citizens, as writers, and as those who are listening to what is going on around them today. One of them is today's first speaker, Pulitzer Prize-winner Dana Priest.

For decades, Dana has been paying attention. And she has been doing so, in a word, politely. That is a very hard thing to do. Measured and careful in her observations and judgments, Dana has watched, she has waited, and she has respected the people who she has talked to. As a result, they have returned the respect. And because of that, she has been able



“Secrets are hard to keep in a democracy. It *should* be a contest. Those of us who are engaged in it should not feel discouraged.”

Dana Priest

to get the stories that have been most critical to public awareness, particularly in the last three or four years – in pieces on secret detention, rendition, and most recently the conditions at Walter Reed Army Medical Center. In so doing, Dana has enhanced profoundly our understanding of what has happened in the relationship between knowledge and power, between secrecy and government.

Dana Priest:

Today I am here to talk about Secrets. Secrets with a big “S” involve classified information. Secrets with a small “s” are those in which people risk their jobs and their reputations just by speaking publicly. When you boil it all down, what we are talking about today is a contest here in the United States between the government on one hand and a set of actors on the other. Those actors include the law (judges and lawyers), nongovernmental organizations (especially the human rights organizations since 9/11), the media, some governmental investigators, and Congress.

At times, the rules in which the contest is waged have been skewed by the government *in favor* of the government. That has been the case since 9/11 of course. One side, the government side, has had a huge advantage. But all governments try to keep secrets. Remember Bill Clinton’s healthcare task force. It sounds like a small thing now, but at the time we were all outraged that it was conducted in secret and that litigation was required to tell us who the members of that task force were.

So let’s talk about some of the actors on the other side for a minute: the journalists. We have had a magnified importance since 9/11, and for journalists that should be very exciting because most of us joined the profession because we think of ourselves as watchdogs.

But the big lesson that I have learned in the last five years, and that I relearn all the time, is the importance of weaning ourselves away from

the center of gravity in Washington. This gravity keeps most reporters near the White House and near government institutions where they get a lot of information, some of it obviously in the form of calculated leaks that are doled out for calculated gain on the part of the government, and some of it actually very important information for journalists to pursue. But it is important to detach from this.

I have learned and relearned this over and over in my career. I have been embedded with the military from time to time, and journalists do get an incredible level of access. But it is detaching from those organizations that has yielded the best results in my own experience – from, for instance, being able to report about the Special Forces’ worldwide program (even before 9/11) that was often counter to the Congress’s wishes, or the secret prisons that the CIA set up, or the rendition program, or even Walter Reed. These were all things that I did as a beat reporter but detached from my beat and detached from many of the government officials who have much of this information.

I was forced to be this way because my last beat was intelligence. That is where I really weaned myself away from any government help, but it is something that I have to remind myself of all the time.

I was reminded of this just last week when there was a message on my answering machine from the U.S. Special Operations Command. For a brief moment I had this fantasy that these guys actually, finally, wanted to play ball. I didn’t even know what it was about. I just thought that I had asked them for something in the past and now they were kind of worried, so they were going to give me some information that they were not going to give me before. So I called up the officer who called me. It turned out to be the Freedom of Information Act officer, who told me that a request I had made nine years ago was ready. He wanted to know whether I was still interested in getting it. Not

knowing what it was, I said, “Yes, of course,” and I asked, “Is it going to be interesting?”

And he said, “I don’t think so.”

So again, I slip into this mode of letting my guard down and sometimes think that I am actually going to get a lot of help. It is good to wean yourself away from that expectation.

When you are dealing in the realm of classified information, all of us as reporters (speaking for *The Washington Post*) take this subject very seriously, maybe even to the point of feeling guilty about getting something that we are going to have to consider whether to publish or not. But I have a note that I’ve tacked up on my cubicle wall to remind me that the government uses classified information in a very heavy-handed, propagandistic way at times. It is a note that was unearthed in the Scooter Libby trial. It is a phone call to Libby on July 10th, 2003, from Mary Matalin, Dick Cheney’s personal communications advisor. It was her plan to discredit Joe Wilson by leaking some damaging information that happened to be classified. And the note on my cubicle wall just says, “We need to be able to get the cable out. Declassified. The president should wave his wand.” His *wand*. Okay. That is something to remember. You know, forget the national security concerns. This is inside the White House.

Another important lesson that I have learned and hope to remember is that storms blow over, and usually fairly quickly. It may not feel that way for those of us in the middle of them, but it does happen. I was reminded of this by my colleague, Walter Pincus, who has a longer history of these things than I do. Last year at this time, I had mailboxes, e-mails, and voicemails full of vitriolic hate mail and some threats, and a public calling for my jailing, all because of the CIA prison story. I had sources who were angry, others who were cold, and others who just did not bother to call and weigh in. People were calling me a traitor. The head of the CIA’s Directorate of Operations flew to

Eastern Europe to hold the hands of the intelligence services there. The president was saying that this was basically going to be the end of our relationships overseas and the end of cooperation. That has not happened.

But this year, because I stumbled onto Walter Reed, the phones are ringing off the hook. Some of the same people are thanking me. Many other people are saying, “Oh, yeah, this is what journalism is all about.”

In between then and now there have been ramifications for the CIA prison stories. There have been huge investigations throughout Europe, in every country – all of the governments have been forced to respond to their citizens and to their legislatures. There are three criminal investigations underway. Europe is publicly setting new limits. There is also a debate in the U.S. government. The president of the United States closed those prisons, no doubt opening others, as we have read about in Ethiopia recently.

So those are the journalists. Things are more mixed on the legal side. There have been challenges to the military tribunals, but overall the claims in the courts for things like the state secrets privilege have been adhered to by judges who (seen from afar with no legal knowledge of my own) seem to be still scared and worried about taking on, turning around, and debating some of the most serious national security issues rather than just doing what the government says. An example of this is the case of Khaled el-Masri, who was wrongly kidnapped. This has been fully disclosed by the German government but our government will not even take up his case because of the state secrets pleading.

More broadly, though, organizations (mainly human rights and civil rights organizations) and lawyers have forced the courts, the public, and the Congress to debate the effectiveness, the morality, and the legitimacy of harsh interrogation techniques, the extent of and limita-

tions on terrorist networks, and the very premise of the creation of a whole set of new laws, rules of engagement, and prisons to hold the terrorists. All sorts of these things have been debated.

Even government investigators and auditors have started digging into the National Security Agency wiretapping program. The Foreign Intelligence Surveillance Court has changed some of the ways that it has been doing business. The Department of Justice has recently revealed that the FBI had improperly obtained telephone logs and banking records for thousands of Americans by the misuse of national security letters.

So what is the scorecard now if secrecy is on one side and the public's right to know is on the other? I think that we know a huge amount about the secret parts of our government's activities in what they call "the war on terror," consisting of things that they began doing after 9/11 that are new, different, and sometimes legally questionable. We were supposed to know none of this but we know a lot.

We know about the extent of special operations and CIA activities; not the details but the framework, the importance of the liaison relationships overseas, and what we are paying some of those governments to engage in it. We know a lot about the detainees – how they have been treated, who they are, and whether they are terrorists. We know a lot about the military's new global reach, and we have a sense of its budget, though a lot of it is classified. We are getting a better sense of terrorist networks – who they are and who they are not. We know a lot about electronic surveillance. Of course this is just a tiny corner but it has begun to crack. We know a lot about the use of national security letters and, finally, the legal framework that came out of the Office of Legal Counsel at the White House – who put it together, why they put it together, what their thinking was, and how it became controversial

within the government itself.

The one big caveat to all this positive news is Iraq. The implications of our collective failure to unearth the secrets about Iraq that the government was hiding will be with us for generations.

The bottom line is that secrets are hard to keep in a democracy. It *should* be a contest. Those of us who are engaged in it should not feel discouraged. We should not feel like the sky is falling. We should feel encouraged that the sky is opening up and that there is a little bit (and in some cases a lot) of sunshine being shed upon these very secret programs. In other cases, the sky is opening slowly and there is still much more to do.

Gaining Perspective: Secrecy Then and Now

Panelists:

Scott Horton, Col. W. Patrick Lang,
Walter Pincus, Michael Sheehan

Moderator:

Prof. Noah Feldman

Prof. Noah Feldman:

There is an economy of secrecy insofar as secrecy is created, shared, passed from person to person, and challenged. Within this very complex economy, there are many different roles. Often the same person will play different roles at different stages of his or her career. Sometimes the same person will play different roles on the same day.

This panel has been carefully composed to reflect varied experiences in engaging the question of secrecy from the perspectives of people who have played very different roles in this complex economy, and in most cases more than one role.

Col. W. Patrick Lang:

My job here today is to lay a few bricks under the conversation. The fact of the matter is that, although not everyone may accept the idea, governments do have to hold some matters in confidence in order to work properly. In the business of diplomatic negotiations, I think that should be obvious. Congresswoman Nancy Pelosi evidently ran into this problem in traveling from Israel to Syria and speaking to the press about things that may have been told to her in confidence. If you do that, you will usually find that diplomatic conversation comes to an end for one reason or another.

If military plans regarding ongoing or future operations involving actual combat are revealed or talked about, then the government's ability to do anything is severely impeded. In

spite of the gross misuse of the phrase "intelligence sources and methods" across the world to cover any kind of desire to keep something secret, there are facts about the ways that the government collects information that do have to be kept in confidence in order for things work at all. I say that just to lay a baseline.

Having said that, I am now going to talk about how grossly this system is abused in many cases. The pattern of secrecy in the executive branch of government (which is where this resides), and especially in the fields of military affairs, intelligence operations, diplomacy, foreign policy, and foreign operations, are all governed by a series of legislative acts and executive branch decisions, often originating in the president's office. These acts and decisions create an authority for marking pieces of paper as being secret in various degrees. The classifications are "confidential," "secret," "top secret," and things compartmented greatly above that.

This authority is delegated down through the departments of government – in my experience, through the secretary of defense – which further delegate it below. It goes down and down until finally some very junior people end up with the authority to make pieces of information secret (or "classified," if you like). You get to the point at which a junior clerk in a military attaché office in Bolivia, marking up a piece of paper about a conversation that a military attaché had at a cocktail party at somebody's embassy the night before, looks at the paper and says, "This looks secret to me." So that gets typed on the message form and it goes out and becomes secret for all the world because only the originator has the ability to declassify it except through rather obscure bureaucratic processes. As things work in the government, you end up with thousands of people who have the ability to classify pieces of paper.

Complicating this even further, classified pieces of paper kept as permanent records in safes somewhere are required to be held as a matter of record and must have a chain of receipts. But message forms that come in across a teletype machine or electronic business, as long as they are kept in a secure way, never have to be made a matter of permanent record, so there is no bureaucratic penalty paid for just keeping these things forever and classifying more and more of them.

If you work at any real level of sophistication in the executive branch with regard to this kind of thing, you normally work in a space or a suite of offices which is like a giant safe in itself. It has alarms and doors that are secured. As long as you keep those pieces of paper that came in as messages inside and don't make them permanent, supposedly, and you only talk to people who have similar clearances, then you never have to pay any kind of bureaucratic penalty in terms of work for having them. So you end up with thousands and thousands of pieces of paper that are supposedly classified.

As I happened to have had the authority to classify millions of pieces of paper and often yielded to the temptation to do so, I can tell you that the temptation to simply decide that something is secret and to keep it around forever is overwhelming. If you do that, you are covered, as the expression goes in Washington. A decision that that this cocktail party conversation at the embassy in Bolivia (which has a tiny chance of being related to something else) is not worthy of being classified could be criticized at some point in the future. So the overwhelming tendency is for people to simply mark these things as secret in one of the degrees of classification. You then end up with a huge amount of classified paper and reports circulating in the



“The temptation is to just make everything secret; to not run the risk of future criticism entailed in not classifying something.”

Col. W. Patrick Lang

government, either in safes inside secured areas or inside networked systems of computers that link together the various departments of government. There is no bureaucratic penalty for that.

The temptation is to just make everything secret; to not run the risk of future criticism entailed

in not classifying something.

What happens over a long period of time – and it has been a long period of time now – is that a culture arises in the executive branch in which people automatically make things secret that do not need to be secret for any reason whatsoever. Contained within this vast body of overclassified information is a small amount of information that really does need to be classified. But the prevailing culture in these parts of the government which says, “Let’s just classify this stuff and make sure that we don’t have to worry about it,” becomes so pervasive that there is a current assumption that everything the government does is secret, basically. That is the underlying assumption.

I have seen people sit and worry for 25 minutes over making a decision to write an unclassified intelligence information report from the field. Once you get to have a culture like this which assumes that everything the government does is secret, you end up with people unwilling to tell the public anything that they are not required to. You end up with ridiculous situations like the officer at Special Operations Command telling Dana Priest that they are finally going to grant her 9-year-old request for some trivial piece of information that they have probably redacted the hell out of with blacked-out places all through it. It makes absolutely no sense whatsoever.

The climate makes it very easy for people to start to conceal things that they do not want

in the public arena by simply saying, “Well, you know, isn’t this obviously secret? Isn’t it confidential or something like that?” People start classifying information that they want to conceal because it is embarrassing, or because it is politically difficult, or because they aren’t sure about it, or for an opportunity to manipulate the situation in some way.

You end up doing all those kinds of things based on a system that is just completely out of control, which classifies 90 to 95 percent of all the things that they handle. Far too much is classified, so you end up in a situation like the one we have.

Scott Horton:

I have worked in the former Soviet Union. I was deeply involved there for more than two decades, monitoring and covering secret trials and prosecutions. I represented a very prominent nuclear physicist, in fact. Over the last five years, I have time and again witnessed speeches by representatives of our government. They have made statements about their notion of state secrecy. I’ve paused and thought, “I’ve heard this before.” Except that I had previously heard it in Russian. I was shocked to hear it come out of the lips of an official of my government, in English.

Today I am going to talk about why I think that many of the developments that we see going on in our country represent a dramatic rupture with our legal tradition and culture. I am going to go back and talk about the 17th century in England because many of the things that are going on today in the United States are a revisiting of legal issues that were very well settled in that period of time.

In particular, I want to talk about one man. His name was Freeborn John, or John Lilburne. He was a person of little formal education. He became a firebrand pamphleteer (today we

might call him an opinion journalist) among Puritans in the years of the civil war. He had republican sentiments. But, more to the point, he was a very sharp critic of the justice system. He wrote constantly, complaining of aspects of the system that were unjust. He was particularly outraged by the use of the king’s courts to persecute the “dissenters” (the term that Anglicans used to refer to Puritans, Calvinists, Baptists, and Quakers, not to mention the real terrorists of that age, who of course were the Catholics).

Lilburne had been convicted in the Star Chamber in 1638 on charges of importation and dissemination of religious pamphlets which had not been registered (England had a severe censorship regime at that point). He wrote a very compelling account of his treatment. He had been in prison for refusing to answer questions. He was flogged, pilloried, and gagged. He also

described in great detail how highly coercive interrogation techniques were used on him to extract a confession, how he was denied the right of confrontation in his trial, and about the fact that the judges who heard his case were all political figures who had been placed there to do the king’s bidding. The Star Chamber was to Lilburne’s age what the military commissions are to ours. His account was an instant best-seller and it provided much of the impetus for the abolition of the Star Chamber by the Long Parliament in 1641. As *Uncle Tom’s Cabin* was to the issue of abolition, Lilburne’s book was to habeas corpus and the Star Chamber.

He served with distinction as an officer during the civil war fighting against king for country. Afterwards, his advocacy of republican virtues irritated Oliver Cromwell, the Lord Protector, causing him discomfort. Then at length Cromwell decided that it was time to silence Lilburne by charging him with treason.



**“Secrecy and torture
fit together hand-in-glove.
Where one is used, the other
is indispensable.”**

Scott Horton

The trial convened in October 1649. Lilburne was a popular figure in London and he was well aware of this fact. So, when the court proceedings commenced behind closed doors in the Painted Chamber of Westminster, Lilburne opened his answer to the charges read in court with these famous words, “The first fundamental liberty of an Englishman is that all courts of justice always ought to be free and open for all sorts of peaceable people to see, behold, and hear, and have free access unto, and no man whatsoever ought to be tried in holes or corners or in any place where the gates are shut and barred.”

He was raising a direct challenge to the reputation of the Commonwealth courts. He was asking whether the most serious of abuses of the Stuart courts, the abuse of secrecy, would be continued. The court fully understood this challenge. It relented. It ordered the doors to the courtroom to be opened and unbarred. A number of historians have written that the doors were open from that point in 1649 forward.

The judge said, “All the world may know with what candor and justice the court does proceed.”

In the balance of that remarkable case, Lilburne established a number of other privileges. The prisoner in the dock was to be treated with dignity and respect, not dragged before the court in manacles and an orange jumpsuit. There were to be no *ex parte* communications between counsel and the court. Lilburne was to have a right to confront all evidence against him, and there could be no secret evidence. The public was also to hear it and to form its own opinion as to the quality of the justice dispensed by the court. He was guaranteed a right of counsel. Indeed, this is the first time in English legal annals that the right of counsel was guaranteed for the presentation of facts as well as for legal argument.

The fairness of the proceedings had its limits. The judge charged the jury that they must convict, saying, “Never was there a like treason

hatched in the history of England.” But the vigor of Lilburne’s defense was impressive, and the jury returned a verdict of acquittal. So the *Lilburne* case sums up the most significant of what came to be called the Commonwealth reforms of criminal procedure, and the most significant of those reforms was the banishment of secrecy.

Secrecy was what the Roundheads found most odious about the Stuart monarchs’ justice. Certainly, there were unjust practices from this period that came to our country; indeed we can not forget the Salem witch trials. But we should not forget that our tradition stands with the tradition of the Roundheads and their reforms, a part of England in that period.

These practices that were viewed by the Roundheads as the very definition of tyrannical injustice – the practice of secret courts, the use of torture to secure confessions, the receipt of secret evidence, the exclusion of the public from the proceedings, the offering of evidence in the form of summaries delivered to judges without the defendant being able to confront the evidence or to conduct a cross-examination – were considered banished 100 years and more before the Americans rose up in their revolution.

Today, secrecy has reemerged, just as torture has made its comeback, justified on the public stage by government officials for the first time since the famous gathering in the Inns of Court in 1629 in which the judges declared upon their and their nation’s honor that torture was not permitted by the common law.

Secrecy and torture fit together hand-in-glove. Where one is used, the other is indispensable. Torture is no longer a tool of statecraft. Today it is a tool of criminals, although sometimes a tool of criminals purporting to conduct the affairs of state. Having resorted to these “dark arts,” in Dick Cheney’s phrase, the torturers now have the dilemma faced so frequently by criminals. They seek to cover it up. And so the path flows from torture to secrecy, the twin

dark stars of the tyrannical state.

If we look quickly over the proceedings down in Guantanamo that have held the world's attention in late March and early April 2007, we see what secrecy is all about. I ask everyone to pick up the transcript of the Combat Status Review Tribunal involving Abd al-Rahim al Nashiri and to look at where the redactions and censorship occur. In every single instance, they are evoked to obscure acts of torture perpetrated on the defendant. Let us consider: Would there be any need to use censorship with respect to these allegations *unless they were true*? No. Indeed, the fact that they are censored should be taken as an admission. No meaningful effort is made to refute any of the detainee's contentions. No records are spread out showing that he was not tortured. Why might that be?

Let us also focus on the repeated disappearance of evidence, on the fact that two dozen copies of DVDs of interrogation sessions involving Jose Padilla have disappeared without a trace. Let us look at the case of David Hicks, where a plea bargain was negotiated. Again, we see that the principal objective of the plea bargain is gagging, to silence Mr. Hicks so he will not describe his treatment in any way.

On April 27, 1961, John F. Kennedy gave a speech at the Waldorf-Astoria to the American Newspaper Association. "The very word 'secrecy' is repugnant in a free and open society," Kennedy said:

and we are, as a people, inherently and historically opposed to secret societies, to secret oaths, and to secret proceedings. We decided long ago that the dangers of excessive and unwarranted concealment of pertinent facts outweigh the dangers which are cited to justify it. . . . and there is very grave danger that an announced need for increased security will be seized upon by those anxious to expand its meaning to the very limits of official censorship and concealment.

I believe that the moment, the day of official censorship and concealment that Kennedy foresaw, is drawing near – indeed, it is upon us today in America. This moment has crept up on us by stealth and as a result of decisions taken at the highest level of government. These decisions have been made behind closed doors with no public discussion, and with a concerted effort to misdirect the public as to the gravity of the changes in policy which have been undertaken. They have led to a dramatic expansion of the government's action without oversight.

We have a duty to posterity to bear witness to these events. We must document them carefully. We must act to avoid the destruction of valuable evidence and recognize, as we have already seen, that it is in the character of those who commit crimes, particularly crimes involving torture, to destroy the evidence of their misdeeds.

Michael Sheehan:

When Karen initially asked me to participate in this conference, my first flippant response was, "Why are we talking about secrets? There are no secrets in Washington." I still basically hold to that point of view, but there are temporarily held pieces of information that eventually get out that are very important. Some are held longer than others and not shared for other purposes.

Obviously, all nations hold secrets. Two examples are probably the most famous in U.S. history. In terms of military operations, there was Dwight D. Eisenhower's D-Day secret regarding which day he was going to land and on which beach. The fate of Europe for the next several years hung on the secrecy around that deployment. On the diplomatic side, you can think of Henry Kissinger's secret trip from Pakistan to China, which paved the way for the eventual meetings between Richard Nixon, Chou En-lai, and Mao Zedong. Kissinger was not only trying to protect that trip from the Soviet Union and their meddling in it, but also

from our allies such as the U.K. and Japan, who were kept in the dark about that initiative. So, sometimes secrecy – whether in military or diplomatic channels – can be very important, with the fate of major issues lying in the balance.

I think, though, that the greatest masters of secrecy in the 20th century were three individuals: Adolf Hitler, Joseph Stalin, and Mao. I think that these three people were able to have secrecy *of state* that enabled them to slaughter tens of millions of people and get away with it.

Hitler, of course, slaughtered about 6 million Jews over a period of about three years and was able to get away with it. His evil was obviously discovered prior to the end of the war, but completely uncovered afterwards. But Stalin and Mao were able to massacre millions of their population over many years and obscure it in secrecy and lies. Even to this day, we are still finding out the depths of their depravations and what they did to their own populations, particularly Mao. At the same time, we were engaged in that rapprochement with Kissinger’s trip to China.

So there are different levels of secrecy; the secrecies involved in discrete acts and the secrecies involved in entire state actions.

But to get back to what we are concerned with today, we are talking about issues involving counterterrorism and some of the programs involved. I think that most people would agree that the government needs to keep certain secrets. The issues really revolve around programs, not secrets – secret *programs*. Three of them have been mentioned here today: the NSA wiretap program, which President Bush initiated after September 11th; the national security



“Intelligence instruments are crucial to finding and defeating terrorists.... The keys to their success are having strong internal oversights... and making sure the inspector-general systems retain their independence.”

Michael Sheehan

letter program that has been internally investigated by the FBI; and the NYPD programs looking at some of the actions prior to the Republican National Convention here in New York City.

In my view, each one of these programs was justified in itself and was generally well-needed. But each of them probably suffered a little from not getting the proper legislative action and oversight to prevent abuse.

The NSA wiretap program, which we wrote about here at the Center on Law and Security, was in my view well-warranted, and the president should have gotten the proper authority from the Congress. And he would have gotten it. I believe that if he had partnered with the Congress to give them aggressive oversight, he would have gotten that also. I believe that both sides of the aisle would have been able to provide constructive oversight of that program, and it would have worked much better. Perhaps the program would not have been in the jeopardy that it is in right now, although it still is going on. You do not hear a lot of squawking from the Democratically-controlled Congress because they recognize its value. Now, with proper oversight, I think they are a little bit more comfortable with it.

Regarding the national security letters, the abuse was uncovered internally by the FBI inspector general saying that agents conducting investigations had used the national security letters, which are similar to subpoenas, to get phone records of who people had called. As a counterterrorism official, I can tell you that this is extremely important information. A higher level of authority would be needed to listen to a phone conversation. A warrant would be needed

for that. But there is a lower standard for the phone records, which are a very important tool for people investigating counterterrorism issues in the United States and abroad. I hope and believe that the program will survive, but there is going to be more scrutiny and oversight both inside the FBI and by the congressional watchdogs, the press, nongovernmental organizations, and others.

In terms of the NYPD programs that were scrutinized by *The New York Times*, I think that these are very good programs. They just need to make sure, both internally and externally, that there is oversight to prevent abuse.

I firmly believe that intelligence instruments are crucial to finding and defeating the domestic and international terrorists who are conspiring to harm the American people.

The keys to their success are having strong internal oversights by bureaucrats who are generally not beholden to political parties and making sure that the inspector-general systems within these agencies retain their independence. The Congress and the press can help do that.

The Congress must remain vigilant and aggressive. I think that the Congress basically laid down on its back between 2002 and 2005. Even though it might have been a majority Congress with some minority, I think that there was a tremendous lack of due diligence on their part in making sure that the administration did not abuse the powers that were given to it after September 11th. I think that the Congress is aggressively trying to get back into it right now.

I also believe that it is very helpful to have split government. When you do not have split government, whether you have Democrats or Republicans in charge of the executive branch

and the Congress, it is much more difficult to adhere to accountability standards. But not impossible. Even a minority in the legislature has tremendous powers over the other party in the executive branch. They just have to know how to exercise those powers and how to use the access that they have in the committees to get information.

The second issue that I would like to raise is an important factor that is sometimes not

inherent in particular programs but rather in how information is leaked. I will give you a quick example of how selective leaks give the executive branch tremendous power.

Leading up to the Republican National Convention in 2004, there was the case of documents showing that a captured terrorist, Abu Issa al-Hindi, was conducting surveillance on certain buildings in and around New York

City – the Citigroup building at 53rd Street and Lexington Avenue, the Prudential building in Newark, New Jersey, and the International Monetary Fund building in Washington, D.C.

The alert level went up to orange, and there was a tremendous amount of concern about the buildings that were surveilled. After about two days of looking at that intelligence, I realized that it was old and not that important. I was asked by several people, journalists and people from both presidential campaigns, whether this had been exaggerated. I looked carefully at the statements that were made and I had to say no. Everything said by Governor Tom Ridge and the Department of Homeland Security was accurate. It was hard to punch a hole in it. But, at the end of day, I looked back at it and said that it was probably an exaggeration. I do not think that Governor Ridge did that on purpose,



“We have a well-earned reputation among many of our partners overseas for a complete inability to keep a secret. That reputation undermines us now, and will undermine us in the future.”

Michael Sheehan

but the selective gathering and distribution of information can be very powerful.

The other classic instance of this was Secretary of State Colin Powell's briefing to the United Nations on the eve of the Iraq War.

The challenge for those who have access to this information and who are watching things unfold, such as Secretary Powell at the United Nations or Governor Ridge raising the threat level to orange, is how to confront the problem when they do not control the levers that determine what can be released. Only the executive branch controls those levers; what Dana Priest described as waving the "wand." It is the executive branch that can release certain bits of information.

When Governor Ridge went forward with the names of those four buildings, he was releasing classified information. I knew that releasing the names of those buildings meant that the operative who had done that reconnaissance knew immediately that his cover was blown (he had not been arrested at the time). I was watching this and saw that pieces that would have given a little bit more context had not been released. There was nothing wrong in what he put out, and I might have done the same thing if I were in his shoes, regardless of the political environment.

But there is a responsibility on those in Congress who have the information. They could read all of those documents and make an effort to round out the story.

Walter Pincus:

There are two elements of my background that I would like to mention to begin with. The first is that I was drafted into the Army at the end of the Korean War and served in the Counterintelligence Corps.

The lesson that I learned is that classified information is not particularly classified just because it has a stamp on it. Pat Lang laid this out extremely well. The realm of classification has really been demeaned over the years.

Classification of information as secret, top secret, or even beyond is often used as a protective device. There are no penalties for overclassifying anything. The people who know this best are the people inside government. They are the ones who watch the selective leaking that Michael Sheehan has talked about.

Second, I ran two investigations for Senator J. William Fulbright in the Senate Foreign Relations Committee during the 1960s. Those two investigations, particularly one on military and foreign policy, taught me that classification can really be dangerous to public policy. The examples that I always go back to are the bombing in Laos and the invasion, or incursion, into Cambodia.

The bombing in Laos, which was always considered classified, went on for years. The public did not know about it because it was classified. We had to have closed hearings about it. The bombing worried the chairman because we were, in effect, fighting a war and not admitting it. Because he was a fairly rational human being, he wanted to know whom we were keeping it a secret from. The Laotians knew it, the North Vietnamese knew it, the Chinese knew it, and the Russians knew it. The people who did not know it were the Americans.

That was carried to an extreme in May 1970, when the so-called "incursion" of Cambodia took place. I was with the committee at the time. When we first heard about it in a classified form, the government did not intend to announce it. The sending of troops into a third country was not to be announced. There was a big confrontation with the administration, and after 24 hours the chairman finally persuaded the administration to admit what they were doing.

That experience taught me a lesson, which is that secrecy can be used to take on extraordinary activities. If you do not tell anybody, you can then play it the other way, which is to say that the other country is being offensive; that

the other country is doing something that we do not know about.

The North Korean nuclear weapons program is the major example that I've always talked about after it was publicly disclosed. People wonder why North Korea began that program. If you go back in history, you will find out that they went to China for support for it within a year after we secretly deployed nuclear weapons in South Korea.

We finally withdrew those weapons during the Bush administration. We never acknowledge where we have nuclear weapons. In this case, it appeared as though the North Koreans suddenly wanted a nuclear weapon out of the blue. It appeared this way because the American public did not know that we had nuclear weapons in South Korea.

So, that was an early lesson about dealing with secrecy and the problems it entails.

In the 1970s, I was reading a lengthy transcript of a hearing on the U.S. nuclear weapons program before the Appropriations Committee. It had been a closed hearing but the transcript was finally published. In the midst of the discussion, there was mention of finally going ahead with an enhanced radiation weapon. Because I had studied nuclear weapons before, I knew that it was the neutron warhead that we had talked about building and never had. Finally we were going ahead and building it just prior to the Carter administration coming in.

And so I wrote a story about the neutron warhead (not a bomb; it was a warhead for a Lance missile and for 155-millimeter artillery). The story was taken as a great violation of security. The fact of the matter is that I had gone to the generals who had put the program together, and some of the people at the



“Classification of information as secret, top secret, or even beyond is often used as a protective device. There are no penalties for overclassifying anything.”

Walter Pincus

Pentagon were the very people who talked about it in a way that everybody disliked, as a cookie cutter (but the classic description is that it kills people and leaves buildings).

Harold Brown, who was Secretary of Defense then, came in to the *Washington Post* offices to see Ben Bradlee because I had written a second piece. That second piece

said that the warhead was part of a broad plan to use tactical nuclear artillery in Europe. The Europeans were very upset about the regular nuclear weapons we had stored there in the 1950s because using those weapons would have destroyed the land of Western Europe. The neutron warhead supposedly had a lesser effect, although it really did not.

I had to sit in on the meeting as Secretary Brown and his top assistant on atomic affairs complained and said that we had to stop writing about it, while the person who had accompanied Secretary Brown was one of the sources for the information. That did much to shape the way I sort of cynically look at classification.

In the *Wen Ho Lee* case, a scientist at Los Alamos downloaded codes for all of our nuclear weapons, put them on transferable disks, and removed them from the laboratory. Nobody in the history of the labs there had done anything like that. Everybody is fairly sympathetic to Wen Ho Lee because his arrest and other matters were mishandled. You have to remember that he did plead guilty to a felony of misusing classified information. He got off in part because these codes that gave the underpinnings of all of our current nuclear weapons were used *inside* the laboratory. The argument was made, as Pat Lang alluded to, that they were not classified because nobody had access to them. They were on classified computers kept in a classi-

fied zone. The argument was made in court that there were no markings on them. So that is a case of classified information that is not marked but dangerous.

Finally, there is the ongoing *AIPAC* case, in which two civilians have been charged with violating the Espionage Act for passing classified information orally. The information was given to them orally and they passed it orally. This is carrying this administration's view of classification to the ultimate point. The information is not marked, and I think that if and when the trial takes place you will find that this is information that some of us who cover national security talk about every day.

Prof. Noah Feldman:

Before opening the floor for conversation, I would like to offer a thought or two about the different perspectives that we now have in front of us to help set the tone for the day.

One theme that Pat Lang emphasized is the bureaucratic incentives to create secrets and the unnecessary character of that, or the way that the bureaucracy is skewed so that there is an incentive to classify but not to underclassify, or even classify correctly.

Scott Horton sounded the theme of a particular kind of abuse of secrecy; namely the abuse of secrecy to hide illegal action by the government. Scott emphasized the abuse of secrecy to hide torture. A second element in his talk was a concern about the interplay between secrecy on the one hand and trials, with their historical and moral value of publicity, on the other. Those are two interrelated themes.

Michael Sheehan emphasized that to have a secrecy regime inevitably and inherently entails the selective disclosure of information. I think that probably has to be true on any theory of secrets. There is no point in having a secret and keeping it entirely to yourself – that is the very definition of a secret; it is useless if you never communicate it to another person or act on its basis. So having a secrecy regime means selec-

tive disclosure. The question is, when it is appropriate to selectively disclose? In particular, and I think this comes across in the interstices of what Mike Sheehan was saying, what is the line between the political incentives of players to disclose secrets and the “national security” incentives?

I think this balance came through powerfully in Walter Pincus's comments. When one is speaking of war, it can be extraordinarily difficult to disentangle the distinction between the protection of national security interests and the promotion of the particular, perhaps partisan, interests of a government that is in power. I do not mean there is a clear line that people mix up. Often there will be no clear line insofar as fighting a war in a democracy or a republic requires at least the tacit consent of the people. So the strategic decision to pursue war under conditions of secrecy is intertwined with the strategic way that the war is pursued. This remark is not intended as a defense of that but as an observation of the way that secrecy deployment works in war; that the line between politics and national security is not going to be easy to discern.

EXCERPTS FROM THE QUESTION AND ANSWER SESSION

Jon Benjamin (*from the audience*):

I am the British consul in New York dealing quite often with counterterrorism cooperation between Britain and the U.S.; specifically New York and London. Before that, I dealt with counterterrorism issues in the embassy in Washington.

When I joined the British Foreign Service more than 20 years ago, I became familiar with our classification system, which is very similar to that in the U.S. The classifications are unclassified, sensitive, restricted, confidential, secret, and top secret, and there are even classifications above top secret that are so secret that even the

names of those classifications are secret. When I first started in the Foreign Service and was trying to grasp how and when to classify bits of information, the definitions were fairly abstract, and it was not at all apparent to me how I should operate within the system.

Interestingly, those definitions are now much more concrete in the UK. In short, these different levels of classification are defined by how embarrassing or damaging a piece of information would be to our national interest if it were to appear on the front page of the *London Times* or *The New York Times* or *The Washington Post*. Would a piece of information just be embarrassing or would it be damaging to vital interests? The implication is that if it is just embarrassing, then it does not deserve or merit a very high level of classification.

My question to the panel members and to Dana Priest is about how we draw the line. Which types of information really deserve a higher classification? Pat mentioned the content of diplomatic negotiations and military planning. Here in the consulate, we deal regularly with incoming VIPs, from the Prime Minister downwards. We classify their logistical plans because these people are potential terrorism targets.

Specifically to Dana, is there a piece of classified information that you would certainly not publish if it were leaked to you, and how would you decide that?

Dana Priest:

In the case of the CIA secret prisons, we did not publish the names of the countries involved. As we tried to explain to our readers, the government made the argument that those countries were cooperating on other things that we decided would not be considered controversial. We happened to know independently what some of those were. If we were to put the names of those countries in the paper, that cooperation might end. Second, they might be put at risk because the prisons

there held high-value targets.

For Len Downie, who is the executive editor and who makes the decisions on this, political embarrassment and the risks that might entail were not considerations.

I really think that sources and methods and future operations (particularly sources and methods) are the things that we generally do not put in the paper. The problem is that the government calls almost everything sources and methods.

Walter Pincus:

We do not publish stories that we think involve classified information without going to the government. In every instance, we go to the government so they have an opportunity to make their case. Whether we accept it or not is something else again; many times we do.

Prof. Noah Feldman:

Dana and Walter's comments are very interesting because they suggest that if you were to describe the U.S. secrecy system from the outside, you would first have to talk about the bureaucratic structures for formal classification; then about selective disclosure, both leaked and non-leaked; and then lastly you would apparently need to recognize a further level of bureaucratic review by the journalistic institutions as part of our system.

The review by journalistic institutions raises the question of the identity of the person to whom the leak occurs. If someone leaks to *The Washington Post*, that means there will be a further level of bureaucratic analysis by specific people within the newspaper according to a process that may not be written down exactly, but which is probably very well understood by the participants. In that analysis, an independent, public policy-oriented decision would be made by people who are not elected, who are not democratically responsible, who are not particularly legally constrained, and who are going to act on the basis presumably of what they

think is their conception of the national interest. That is an extremely interesting way of thinking about the problem.

Michael Sheehan:

I'd like to put in a plug for tightened secrecy and security within the U.S. government. We have a very well-earned reputation among many of our partners overseas for a complete inability to keep a secret. That reputation undermines us now, and will undermine us in the future when we need to conduct a sensitive operation with a partner country that decides not to cooperate with us because they know that eventually it will be in *The New York Times* or *The Washington Post*.

I believe that this is dangerous. I'll give a hypothetical example of incidents which happen all the time. Country X arrests a terrorist. They do not share that information with the CIA because they are afraid that the Americans will take it straight to the press. So they keep it away from the U.S. government for as long as they possibly can in order to conclude their own investigation. When you capture one terrorist, you would like to capture more and more. You often do not want it known that a terrorist has been captured because you are trying to roll up the cell.

The problem is that the Americans will often have information that can help a country roll up a cell more effectively, but that country will not share the information because they are afraid it will go into the newspaper. Opportunities can be lost that way.

Lawrence Wright (*from the audience*):

We have a method of redress in this country for secrets: the Freedom of Information Act. But it has become so corrupted that it is a joke. Dana Priest's experience is not unusual; every reporter has run into this.

Jamal Khalifa, Osama bin Laden's brother-in-law, was murdered a couple of months ago. I received a Freedom of Information brief. It was

six pages long, and only 10 words were not redacted. Eight of the 10 words were either "Jamal" or "Khalifa." At least the information was timely. But it was worthless.

Secrecy and Decision-Making

Panelists:

Barton Gellman, Prof. Jack Goldsmith,
Prof. Stephen Holmes

Moderator:

Prof. Richard Pildes



Prof. Jack Goldsmith, Prof. Richard Pildes and Prof. Stephen Holmes.
Photo by Dan Creighton.

Prof. Stephen Holmes:

Daniel Patrick Moynihan's 1998 book, *Secrecy: The American Experience*, focuses on the pathological effects of secrecy. What I would like to do is discuss Senator Moynihan's claims in light of the experience of the past six years. In the book, he says that secrecy has had an observable effect on government decision-making in the 20th century. His basic thesis is that some degree of government secrecy is necessary but the "culture of secrecy," as he calls it, can do grave damage to national security.

He does have plentiful discussions of the comic aspects of over-redacting. He mentions that a passage from Dwight Eisenhower's published memoirs was redacted out of memoirs written by a former CIA officer. So there is a

good deal of silliness. But it is not all silly.

One thing that I am not going to talk about at length, but which would be worth further discussion, is Moynihan's claim that excessive secrecy has a terribly harmful effect on democracy. When citizens see the government deceiving them, lying to them, and blacking out what

is going on, this foments a kind of irrational culture of rumor and conspiracy-thinking that is very damaging.

But Moynihan's main claim is cognitive. It has to do with how the danger of false certainty thrives behind the veil of secrecy, and how highly insulated policy makers, who are not kept alert and informed by individuals with different points of view, and whose errors are carefully shrouded from criticism and scrutiny, are extremely unlikely to design intelligent policies. The point here is not

about civil liberties but about destroying the forms of public scrutiny that can force a government to give plausible reasons for its actions. A government that is not forced to do so regularly is likely soon to have only confused reasons, or perhaps no reasons, for its conduct. It will begin to rely unduly on untested hunches. If the factual premises of its decisions to use lethal force are not tested by some kind of adversarial process, it is unlikely that the consequences for national security will be favorable.

Moynihan was not thinking about the current administration of course, but his claim has an eerie relevance. The basic one is this: the U.S. government has frequently failed to assess its enemy accurately and to deal rationally with the threats facing it, and one of the principal

causes of that inaccurate assessment is excessive secrecy.

He is not saying that secrecy is unnecessary. Pat Lang's comments this morning about the necessity of secrecy are very close to Moynihan's. Vice President Dick Cheney said that he could not get "unvarnished advice" about American energy policy unless the American energy companies who talk to him are anonymous. That sounds self-serving, and it obviously is, but there is a core of truth in his comment. Confidentiality does have its functions. There is such a thing as excessive, paralyzing oversight, and total transparency is not realistic – as Michael Sheehan mentioned, the plans for D-Day had to remain secret. So it is, all told, a matter of balance.

Moynihan's claim is that denying the public, the Congress, and the press the right to examine and criticize the government has the potential to severely damage national security. Among other things, it can destroy presidents. The effect of secrecy on a president was one of Moynihan's interests, including Richard Nixon's obsession with leaks and paranoia about breached secrecy, even on unimportant matters. Just a few weeks after the Supreme Court ruled that *The New York Times* could publish the Pentagon Papers, Nixon formed the "plumbers" in a fit of self-destruction and obsession with secrecy.

Moynihan cites from a congressional committee in the '60s, saying that secrecy is the last refuge of incompetence. That is meant to be a nonpartisan concept. The background idea is that people behave differently when they are observed as opposed to when they are unobserved. Let's put it this way – we do not invariably behave more honorably or prudently when we are unobserved. This does not mean that transparency is going to solve all problems or make us all honorable. All that I think we need – and this is Moynihan's premise – for a nonpartisan discussion of this issue is to admit that in some cases covert actions may be utterly idiotic. All we need for a discussion is to say that

the publication by investigative journalists of information that the current administration desperately wants to keep hidden can sometimes increase national security. As long as you can say that, then there can be a discussion of where to draw the line, how to do it, and what form it should take. But it takes away the mystique of secrecy and the assertion that there is never a justification for breaching the current administration's claim that what it wants to keep secret is being kept secret for purposes of protecting the nation.

I am going to talk about four points that Moynihan makes. I expect that those here who have more government experience, and those who have been observing government, can modify, deny, or confirm these claims. The four points have to do with cognition, psychology, turf wars, and partisanship.

The first point concerns bureaucracy, and what Moynihan calls "organizational aggrandizement." Bureaucracies get into ruts which they have trouble getting out of. Secrecy exacerbates their tendency to apply old and obsolete solutions, even to new problems. Moynihan cites Max Weber, and Weber's point was that the German *Beamten* was responsible for Germany's terrible failure in World War I because it got in the way of pursuing the war. If the political system were more lively, more partisan, if it had an influence and had been able to jog them out of their rut, Germany would have been in a better position.

This is an important way to think about secrecy because it contradicts the current administration's claim that executive discretion that is unobserved, unchecked by legislative and judicial authority, is more flexible – the claim that, in order to obtain the requisite flexibility to deal with a threat, the executive needs to act in secrecy. What we actually see is that the more the administration acts in secrecy, the more it is stuck in a rut. It has lashed itself to a failed policy and cannot correct itself. That suggests the Bavarian point, which is that openness has

something to do with correcting errors. An adversarial system, in which agencies are forced to admit when they have made mistakes, is more likely to occur where there is a divided government, as Mike Sheehan said. A pampered and unchecked executive can become catastrophically disconnected from reality because it is not hearing and will refuse to listen to bad news. It is insulated. There is an echo chamber effect. Moynihan discusses this under the title “A Culture of Secrecy.”

Second, bureaucrats treat secrets as if they were private property. Noah Feldman said that this morning. A secret is what you tell one person at a time. Moynihan adds that a secret is what you tell one person at a time for consideration, for an exchange. Bureaucrats gather secrets. They say, “The secret is an asset. I need to get something for the secret I have. I will hold onto it until I can trade it for something I need.” The consequences of that are multiple.

The first consequence is that decision-makers are making decisions in the absence of knowledge they need. That would be the primary cognitive consequence. Mercenary or lunatic informants can insert fallacious information into a system that does not have any checks or a way of weeding out this disinformation. Deliberate disinformation is almost invited once you are told that no one is going to double-check it, no one is going to look at it, no one is going to know the source. The source is not being screened. So those sources who do not want to be screened are going to be coming forward out of the woodwork.

Moynihan says that secret information is about as reliable as corridor gossip. That is not always true, but it has enough truth to be worth thinking about. Schemes hatched in secrecy are



“The problem is not simply secrecy and the solution is not transparency. The problem is the lack of any form of adversarial process.”

Prof. Stephen Holmes

frequently addled, he says. Secrecy permits, for example, the decision to intervene militarily in a country about which we know nothing without considering the potential downsides of such intervention. Because there are people who, if they were outside the system, would say, “Look, if you do that” Moynihan was thinking of

Cuba. There was public knowledge that Castro was very popular but the secret decision to invade the Bay of Pigs was done without any kind of obligatory consultations or listening to those outside who might have had something to say about it. By focusing particularly on public liberty (meaning the liberty to examine your government), Moynihan manages to twist and make us rethink the contrast, or polarity, between liberty and security. It might make sense to say we have to reduce private liberty to have more security. But it does not make sense to say that we are going to be more secure if we can prevent our government’s mistakes from ever being revealed, that we are more secure if we can prevent the government from being criticized.

More psychologically, Moynihan and others (including Georg Simmel, who wrote wonderful essays on secrecy) have written about the overestimation of the importance of secret information – the psychology, the spell of secrecy, the allure of secrecy, the ability to say, “I have a secret you do not know about. It makes me feel important.” Dana Priest mentioned this too. There is an overestimation of the catastrophic consequences of disclosure, the sense that “the secret makes me feel so important. If everyone had it, I would feel less important. So, therefore, it must be a very vital piece of information.” Moynihan’s claim is that we overestimate the value of secrets and downplay the impor-

tance of information that is public. This is the Bay of Pigs example again, where he says, almost, that if the Princeton study showing how popular Castro was had been kept secret it would have taken it into account. But it was public, so they ignored it, because you overvalue information that is secret. He cites George F. Kennan at length, saying that 95 percent of the information we need is in the public record. What we need is not disclosure of secrets but analysis.

In the national security area, Malcolm Gladwell's distinction between puzzle and mystery is a good one. A puzzle is something where you have all the pieces of information except for one. If you find the one thing, then everything makes sense. But usually we are in a different situation, more like a mystery, in which you have all the information. You need to interpret it. You need to analyze it. You need to understand it. Stealing a secret is much less likely to get you where you want to be than understanding the situation, which requires investment – not in stealing secrets, but in analysis. Moynihan talks here about the Bharatiya Janata Party's election brochures in India. It was announced that India was going to go for an atomic bomb. That was in the public record but the U.S. administration did not read it. They only looked at their secret information, so they did not predict it. They also overestimated Soviet strength. That is one of Moynihan's main claims. The overestimation was caused, he said, by too much secrecy, by not being open enough to those outside the government.

Third, incoherence within the executive branch is another product of the culture of non-cooperation among bureaucrats, of information-hoarding and so on. Congress and the press get tips from dissidents within the executive branch. We have heard that and it could be the military or others. So keeping secrets from Congress and the press requires the executive branch to keep secrets from itself. That can have terrible consequences if the left hand does not know what the

right hand is doing. Moynihan talks about the dispersal of secrecy centers within the government. There is a very important idea that you have different clumps of secrets. Executive agencies, each with their own agenda – maybe each competing for a part of the action – are not cooperating. We know a lot about this; they cannot cooperate in a master plan. This is part of what the fog and the haze of secrecy is about.

The most dramatic part of this, which speaks to the question of the unitary executive, is the number of cases in which the president is not informed by executive agencies of essential information. Moynihan focused on the Venona decrypts – the fact that in 1946, after the war, the military cracked the Soviet code and decided not to tell Harry Truman. Truman did not know, and he was listening to criticism by conservatives of the Democrats saying, "You are just sheltering communism." He thought they were just partisan attacks. The military and the intelligence agency had the information and didn't tell him. So what does "executive responsibility" mean in a system where executive agencies do not tell the president essential information? That is an important factor to think through.

Finally, I want to say a few words about partisanship. We have talked a little about selective classification and selective leaking for partisan reasons. I have a good example of how partisanship plays into this from Moynihan's book. In 1965, a representative from the 13th Congressional District in Illinois "introduced legislation to establish a presumption that, with only narrow exceptions, executive-branch documents should be available to the public and that judicial review should be available as a check on agency decisions to withhold information." You should not invoke executive privilege to deny the release of documents. That was Representative Donald Rumsfeld who claimed this.

So partisanship is important in making determinations about secrecy. I tend to sympa-

thize with what I thought Noah Feldman was suggesting this morning, that the blurring is almost inevitable. In some way, at certain points, it seems cynical and contemptible. Incumbents in power will say, “Revealing a secret that would embarrass us is actually damaging to national security, because it would embolden our enemies to know how incompetent we are.” That sounds fairly absurd but there is something to this. It is a very complicated area and requires a little more thought.

I’d like to make one final point. In a way, it is elaborating on what Mike Sheehan said earlier. The problem is not simply secrecy and the solution is not transparency. The problem is the lack of any form of adversarial process. The problem is an insulated clique making decisions without having to make a case, without having to expose the factual premises of their decision-making to any kind of test. That test can be relatively sheltered. It could be a select committee on intelligence in Congress. It does not have to be public, but it cannot be a test before a body of lapdogs who are simply doing what you tell them to do. Those who are judging you, and to whom you are accountable, have to have some kind of independent source of information.

I think that way of casting the issue shows that the solutions for this are finding some place between the secret and the transparent. In the war on terror, in facing a threat which we have never faced before, it is inevitable that our government is going to make mistakes. So the idea of handing power to a small group of people who are never criticized, who never admit their mistakes, seems to be the worst possible arrangement that we could think of.

Prof. Jack Goldsmith:

First, I am going to talk about the harmful effects of secrecy within the government and inside the executive branch. My remarks will essentially be taking what Stephen Holmes said about the costs of secrecy between the executive branch, the public, and the Congress and apply-

ing it inside the executive branch.

In regard to Donald Rumsfeld, I do not know what his stated public position about secrecy was while he was the secretary of defense, but inside the Pentagon (when I worked there for a year) he was constantly complaining about overclassification and why things were so secret. He was constantly berating people below him about that. At least inside the Department of Defense, he seemed to have a skeptical attitude toward secrecy. But I do not know what his public posture was.

In regard to the points that Stephen Holmes made, I think that this is a hard problem because there are obvious costs. No one who has worked in the government and who looked at classified information can come away from that experience and think anything but that there is way too much that is secret, that classification is exaggerated. You see how, as Pat Lang said, the incentives to classify are powerful, and you can rarely get in trouble for overclassifying. But you can get in trouble for underclassifying. A risk-averse bureaucrat will tend to overclassify. Then there is, of course, the convenience of classification because, as Stephen Holmes and others have suggested, you avoid scrutiny, you avoid your judgments being exposed to debate and to review. You get less disagreement. And in some sense you get, as Noah Feldman started off suggesting and as many others have said, more power by controlling the information.

So there are many incentives for any executive branch official – and, by the way, for many government officials outside the executive branch, including in Congress, the courts, and other bureaucratic institutions – to keep things secret. In the executive branch, I think it is obvious that there is way too much secrecy. As Stephen Holmes and others have suggested, the costs of secrecy are well-known. Daniel Patrick Moynihan’s book is great on this. Decisions based on skewed or incomplete information are not very good. Errors get hidden, they do not get exposed, there is less accountability. You do

not get to correct mistakes because you do not learn about them; you do not achieve all of the benefits of deliberation and argument.

The hard question, of course – and I think that everything I just said is true, and in that sense I agree with Stephen Holmes – is knowing where the line should be drawn. I am still talking here about the line between the executive branch and other actors. I think it is a very hard question, because there are clear benefits, as everyone acknowledges, about secrecy, especially in deliberation but less so for final decisions. I think the justification is a heightened one for final decisions.

I want to talk briefly about secrecy inside the government, and between agencies, because one of the things I took away from my government experience is that all of the pathologies of secrecy that occur vis-à-vis the executive branch, Congress, and the public also occur among agencies and among individuals inside the government. The same incentives appear and are exacerbated by the fact that each agency does its own classifying and does its own screening for who gets access to classified information.

When we talk about the information-sharing problem inside the government that everyone has been talking about since 9/11, it is not solely, or even primarily, about bad computers and bad databases. It is about bureaucrats having powerful incentives not to share information with one another. We have seen this in many of the errors that the administration has made. The same mistakes that secrecy produces vis-à-vis the public also occur within the executive branch.

I will give a few examples of how secrecy affects lawyers' decisions. I am thinking about

lawyers inside the government performing advisory functions, which is what my job was at the Justice Department. I was the head of the Office of Legal Counsel, advising many different agencies, including the White House, about the legality of actions. What I am about to say is also true of general counsels of different agencies advising the heads of their departments, and lower officials within those agencies advising government clients.

Especially in national security, when there is classified information you sometimes cannot get inputs from the people you think you might want them from, lawyers especially. You want legal input from a certain agency and you cannot get it because they are simply not read into

a program. Believe it or not, if you want to deliberate or try to give a sound answer, it is sometimes very hard to get input from a government lawyer in another part of the bureaucracy on something he or she might have expertise on. You cannot do it because that person is not read into a particular program. Sometimes you cannot get them cleared into

the program even if you are the head of the Office of Legal Counsel and are trying your best. Sometimes you can, sometimes you can't. Sometimes, even if it is not a classified matter, there are reasons – which I never found terribly powerful – that one's clients do not want input from other agencies. So that can be a type of secrecy inside the executive branch that makes deliberation difficult and that I think produces a less satisfactory legal product.

Another type of failure is about facts. Often, when asked to give legal advice on a question, in order to provide good advice you need to know what the facts are and you need to understand the implications of your legal deci-



**“All of the pathologies of
secrecy that occur vis-à-vis
the executive branch,
Congress, and the public also
occur among agencies
and individuals.”**

Prof. Jack Goldsmith

sion. Sometimes, especially in areas of national security, it can be frustratingly difficult to get all of the facts you need to know in order to answer a question. Even when you think you have all of the pertinent facts on which to base a legal judgment, you can find out later that you do not. You don't know what you don't know,



Anthony Lewis, Barton Gellman. *Photo by Dan Creighton.*

obviously. Sometimes facts can be withheld from you on purpose. Sometimes it can be just through some pathological accident, or oversight. But this is another problem of secrecy inside the executive branch and of the culture of secrecy in general that leads to poor deliberation by lawyers, and which can result in sub-optimal legal decisions.

I do not think, and I do not think Stephen Holmes was suggesting, that this is just a problem for the Bush administration. I think that this is part of the culture of the executive branch. It can be better or worse in some administrations. But these are structural problems that persist across administrations. Since the country first began, we have had a long-term secular trend towards increased secrecy inside the executive branch, and between the executive branch and other actors in the government.

I do not have great solutions to this prob-

lem. I am not terribly optimistic that we are going to be able to fix it. Since 9/11, we have been trying like crazy to fix the problem of information-sharing within the executive branch, with only mixed success. At the end of the day, it is the executive branch's problem to fix. For the very reasons we have been discussing, executive branches and their leaders are not usually enlightened enough to fix the problem. They have the immediate incentive to keep things secret, and to keep the system in place.

Barton Gellman:

I would like to play off something that Michael Sheehan said earlier. I will say for the record that I have great respect for him. I think that his statements were very moderate and interesting. I think he may have given a wrong impression, though, on

the subject of national security letters (or "NSLs") and how the problems with those letters became known.

I actually think it is as close to a textbook case as I have ever been involved with, in 18 years at *The Washington Post*, of the interaction between formal government institutions and outside scrutiny, in terms of bringing an issue to light and leaving it to be debated. I happen to know something about this. The whole thing began with Jameel Jaffer and Ann Beeson of the ACLU. They mounted early legal challenges to the constitutionality of the national security letter gag orders, winning important victories in federal courts in Connecticut and New York and pointing the way towards lines of inquiry picked up by *The Washington Post*, Congress, and the Justice Department's inspector general. The catch was that they couldn't disclose much about the cases in public – they, too, were gagged by the Patriot Act. My contribution was

to break through some of the secrecy and tell the public, and Congress, what was really happening. In November of 2005, I did a 5,000-word story on NSLs. The ambition of the story was to take an example of a power that had been added or changed and, four years after the Patriot Act was enacted, to see how it was working, what was being done with it, and what was happening.

Every single thing about it was classified. The government was answering very few questions about national security letters. Until you read the story, you could not have known that there were tens of thousands of them being issued a year, as opposed to a number that had been in the hundreds in the 1990s. The great majority of the people whose information was being culled and sifted through were U.S. citizens or residents who were not suspected – not even not *known*, but not even *suspected* – of being involved in terrorism or in a counterintelligence probe.

There was, essentially, no supervision whatsoever. There was a model memo that was sent out to agents in the field. Agents had to give explanations of why their NSL requests were relevant to a national security investigation. Here is the model for why it was relevant to get someone's phone records: "It is relevant because I want to know who he is calling." That was literally the test used by FBI agents in the field. "I want his phone records because I want to know who he is calling."

Something that has not been discussed publicly almost at all is that there have been almost 200,000 NSLs since the Patriot Act was passed. Everything was sifted in the NSL process – including financial transactions, phone and e-mail records (not the content, but who you e-mail and when), Web addresses that you browse, and full credit histories, which include everyone you have ever lived with and every place you have ever lived and when — and all of that information has been retained. None of it has been thrown away. All of it is in govern-

ment databases, which are, fortunately for people who care about privacy, not very efficient at the moment, but they have the ambition of becoming efficient. Every single thing I just told you was classified at the time I wrote the story.

It may be that we, as a society, are willing to say that this is the balance we are willing to strike between security and privacy in the post-9/11 environment. I believe Mike when he says that this is an enormously valuable tool and that in some percentage of the time you are going to find connections that will lead you to important investigative results. But, as in many other cases, the balance between government power and individual liberty and privacy shifted very substantially after 9/11, and that needs to be discussed.

I wrote the story while Congress was debating the reauthorization of the Patriot Act. National security letters were not among the expiring provisions, so there was no need for Congress to debate them. But members of Congress were irritated to learn from *The Washington Post* that they had been given incorrect data on even the number of national security letters, and that the assurances they had been given that the process was carefully targeted and closely supervised were false. They were simply false. There was literally no supervision and there were dozens of people in power to sign off on these letters.

Congress introduced amendments to the Patriot Act reauthorization. One of them required the inspector general of the Justice Department to investigate the use of NSLs and the degree to which they are supervised, and report to Congress. One of the things my story reported was that the Justice Department had said, "We have an inspector general who could investigate any abuses." The problem with NSLs is that they are automatically, permanently, and unappealably secret from the person whose information is requested. There is almost no chance that Verizon is going to complain to

the Justice Department about a request to give someone's phone records to the government. They have no reason to know whether it is or isn't abusive. The inspector general was quoted in my story as saying, "It is a little bit hard to understand how I would get a complaint to investigate." So Congress said, "investigate."

Fifteen months later, on March 9, 2007, the inspector general came out with a report stating that the numbers are larger, and the supervisory problems greater, than I had known when I wrote my story. You now have an interaction between an executive watchdog and an outside watchdog. There are, meanwhile, several court cases challenging the constitutionality of the gag provision of the NSL. So you now have a significant debate in Congress about where we are going to draw that balance. That is, I think, the way it is supposed to be.

On the other hand, I just told you that I published classified information. So who elected me? What right do I have, or does *The Washington Post* have, to spill secrets that have been stamped with a stamp which states that there will be either harm, serious harm, or exceptionally grave harm to the national security of the United States if they are made public?

My answer is that national security presents a conflict of core values in our society between self-government and self-defense. If we do not know what our government is doing, we cannot hold it accountable. If we do know, our enemies know also and that can be dangerous. Wartime heightens the case for secrecy because the value of security is at its peak. But secrecy is never more damaging to self-government than during wartime because making war is the paradigm of a basic political choice for the country.

My belief is that no individual or institution can be trusted to draw the line for us. Noah Feldman mentioned earlier that the questions involving secrecy have to do with when, and perhaps why, a secret is disclosed. By whom also matters a great deal. There is actually no one that you could trust to draw a balance

between national security and accountability. That certainly includes the people with the classified stamps, but it also includes newspapers.

I am not elected. I am not responsible for national security. I am not sufficiently informed to know, as an expert, what will do damage. On the other hand, political leaders are disqualified from the job of telling us what we need to know in order to hold them accountable at the next election. They are not only likely to draw the line differently than you or I might draw it, but they are not entitled to draw that line because the whole idea of a sovereign people is that we decide what matters to us.

One of the most interesting things, to me, about Daniel Patrick Moynihan's book is his conception of secrecy as a form of regulation. Regulation in domestic affairs normally involves telling people what they may do, and those rules are open. In foreign affairs, and in national security, regulation involves telling people what they may know, or deciding what they may know. Normally, those decisions are not known to the public. So the question becomes: What should be the standard? How do you decide what to publish?

There are several fundamental purposes cited in the Preamble of the Constitution. One of them is national defense, but there are competing virtues in our form of government. So it cannot be enough to say only that a given disclosure would cause harm. Sometimes, that is a good reason for not making the disclosure. But it cannot be that we accept the absolute reverse of the JFK speech, and that we will pay no price, and bear no burden, for the preservation of liberty. You have to say that if both values matter, sometimes it is worth paying a price in potential harm to national security.

Likewise, it is obviously necessary in some cases to say, "We are going to have to withhold this information from the public because there would be too great a harm." As Dana Priest and Walter Pincus alluded to earlier, *The Washington Post* does this all the time. Because

we do not have an official secrets act, in practice the lines between secrecy and disclosure have been drawn by a process of competition. The government tries to keep secrets and we try to find them out. There are intermediaries with a variety of motives who basically perform the equivalent of arbitrage.

Here is the key point. In general, the way it has functioned for the past several decades is that there was no one who exerted coercive power that really worked at the boundaries. If you had access to classified information lawfully, there were rules, contracts, and civil penalties (and potentially criminal penalties, although they were very rarely invoked) for disclosing that information. On the other hand, you were taking a significant career risk. You had to feel that there was a very strong reason to do it. Reporters and publishers at that time (I think it is different now) incurred very few risks. But, as Walter said, we always consult with government when we find out something secret. I have withheld many details from stories, and I would say two entire stories, since 9/11.

I will give you an example of a story that I withheld during the first Gulf War that is now public. I noticed that General Schwarzkopf suddenly, from one week to the next, claimed in the briefings something like a tenfold increase in the numbers of Iraqi tanks and artillery pieces that were being destroyed in the bombing campaign. Of course, you have to be curious, and maybe a little skeptical, when the government suddenly starts claiming enormous increases in success. So I poked around, and with my colleague Rick Atkinson discovered that they had come up with a new, technical way of finding buried armor in hot desert sand – by using infrared sensors to look for cold spots right after sundown, instead of hot spots as they normally do, because armor and sand shed heat at a different rate. We did not even consider publishing that story. It was highly technical. It did not involve a political decision by the people about how we prosecute a war. It would be of obvious

benefit to the enemy to know we knew this, and so on. We did not even need to consult the government. We just withheld it. It came out several years later, in a government-sponsored report actually.

We always have these conversations. We try to strike the balance. We feel that it has to be struck case by case.

Now there are threats to the status quo. First of all, the Bush administration has largely stopped having the kind of constructive conversations in which they would say, “We wish you would not do the story in general, but this is the part we really care about.” In more and more cases at *The Washington Post*, we are finding that the government will simply say, “Do not publish at all. We will not tell you what is more and less important.” They have greatly stepped up their efforts to coerce silence. There is now the routine use of waivers. Government officials are required to sign a waiver of confidentiality, stating that if they ever told a reporter that they want confidentiality when they spoke to the reporter, it is hereby waived. That is compulsory. There is much more use of polygraphs, there are subpoenas, and, in fact, the use of national security letters against reporters. I have good reason to think that, in connection with another story that I wrote, my phone records were obtained by a national security letter. I know that some of my sources were, so that would have led to me in any a case.

There was considerable self-restraint used by government in trying to plumb leaks in past administrations, but that self-restraint has eroded. The status quo is also breaking down in other ways. I think it is dangerous to democracy. It is something that we are having to think very hard about in my business.

Prof. Richard Pildes:

I tend to think institutionally about many of these issues. If you are looking for the sort of adversarial process mentioned by Michael Sheehan and Stephen Holmes, especially during

times of security concern, Congress is the obvious place to look initially for fundamental adversarial conflict with the executive branch. Much more so than journalists, Congress has the capacity – through the subpoena power in particular – to call people in, to conduct hearings, and to generate information. Yet one of the striking things about the early aftermath of September 11th is that Congress was largely dormant during this whole process for four or five years, as Mike Sheehan said. There is an obvious explanation, which is that we had unified party control of Congress and of the White House.

One of my ongoing concerns is how to deal institutionally with unified government in respect to the need for an adversarial process, particularly in these periods. We have not had much unified government in the last 50 years in American politics. Part of what was unique about the post-September 11th environment, politically, was that we had the most sustained period of unified government that we'd had since the Carter administration (when the Democratic Party was a fractious mess anyway, and not unified in any real sense).

One of the ideas I have been working on is whether we should start thinking about devices that would empower the opposition party in Congress do things like conduct hearings, conduct oversight, and issue subpoenas. You can imagine lots of ways in which that would be abused, and the sorts of things it would open up. But if you are serious about Congressional oversight during these periods, you have to think about the problems of unified government and whether there are institutional solutions to deal with them.

People I have spoken to from South Africa and Great Britain talk about the obligation of

the prime minister to meet the opposition in parliament. That is actually far more effective in generating information from the executive than many of us think. Dennis Davis, who is here at the NYU law school, was on the South African Supreme Court. He says that the only time under the prior regime in South Africa that they

would get information about the number of detainees and the like was at that moment. The cultural understanding is that the ministers have to answer, and that the prime minister has to answer. If there are factual misrepresentations, ministers can lose their jobs. They actually have a structure in which the opposition can play a more

effective role, ironically, than our opposition can, even within our nominal system of checks and balances, at least if we are in a period of unified government.

One of the interesting things that has emerged from the comments this morning is that we tend to talk in a very global way about government and secrecy. The discussion so far has pointed out that this adversarial process could occur in many different places in the system. You could have a very intense adversarial process in the executive branch, or not. You could have it between Congress and the executive branch, or not. You can have it with journalists and public opinion more broadly. So, the issue of secrecy has to be thought about more specifically. Is it secrecy within the executive branch from itself, secrecy between the executive branch and Congress, secrecy from public opinion?

I'd like to ask whether this intense adversarial process in the executive branch, if we had it, would suffice. Does the solution require adversarialness between Congress and the president, or just somewhere in the system?



**“National security presents
a conflict of core values
in our society between
self-government
and self-defense.”**

Barton Gellman

Barton Gellman:

It would be hard to argue against the benefit of greater assertiveness and power in all of the coordinate branches of government. I would include not only Congress but also the judiciary, which has had a long-standing post-Cold War doctrine of deference to the executive on issues of national security that has grown substantially since 9/11.

It is much easier to see Congress as a check and a balance on policy, decision-making, and what the United States government will do with its power than it is to see Congress as a check on secrecy. You have the problem of what the epistemologist Donald Rumsfeld called “unknown unknowns.” There is a distinction between “known unknowns” and “unknown unknowns.” If you are buying a used car, a known unknown is that the seller will not tell you what the other bidder is offering. An unknown unknown is that the seller forgot to tell you that the engine fell out last week.

Congress does not have the power to break through the barriers of secrecy, especially on unknown unknowns. Congress has no power to declassify information, even when it considers the information improperly classified. It also does not know anything that the executive branch does not tell it. That can be overt. President Bush, early in his first term, announced that he was withholding all classified briefings from the intelligence committees as punishment for a leak (for which it was not at all evident that Congress was the source). That was a way of demonstrating who’s boss. But there are lots of cases in which the very existence of a program is not told to Congress.

Prof. Jack Goldsmith:

I’d like to give two small examples of how Congress can play an oversight role even when the parties are not split. They took place in the first five years after 9/11. The examples are weak, but I think that they are important.

One is that there is a statutory notification

requirement regarding covert operations and other matters in the executive branch. This seems like a very weak check because, the truth is, the intelligence committees cannot do much once they are notified. They can ask questions, they can express disapproval, but they do not have veto rights and they cannot go public. But it has an effect. Secretary of Defense Robert Gates, in his memoirs, said that when he was the director of the CIA scores of crazy schemes that were hatched in the White House never got off the ground because of the need to go up and tell some other institution what you are going to do. So, in that very weak sense, I think that Congress does have an effect because of the notification requirement, even when it does not want to play an oversight role. That is a good example of how even the weakest of oversight can have a good effect.

When I was in the government, the Democratic senators would send letters to the Justice Department all the time, asking questions. The Justice Department has a policy of answering these questions as a matter of comity. Even though we did not like to because they were often a pain, we did. But here is one modest example of why these questions had good effects. Senators Leahy and Feingold asked a series of questions (this is in the public record somewhere) about the definition of “enemy combatant,” because the administration had not made crystal clear, at least through 2003 or 2004, what the precise definition was, what the process for identifying enemy combatants was, and the like.

We answered those questions. There was an interagency process that took place inside the executive branch to answer them. That process was enormously useful for the government. It was really the first time, in my experience anyway, that there was a government-wide conversation and debate about the definition of “enemy combatant.” In the course of answering those questions, we were forced to deliberate in a way that I thought was extremely useful.

Prof. Stephen Holmes:

Although there is much information hoarding in secret between agencies, and even within agencies, one way to answer the question is to think about how Congress can serve to provide a platform for dissident voices within the executive branch who would be smothered by hierarchy. This could have pathological forms.

Prof. Jack Goldsmith:

That is the problem.

Prof. Stephen Holmes:

It could obviously have problems. But even though Congress itself is not necessarily informed of all those unknown unknowns that Bart talked about, there are people in the executive branch who know about those things. Maybe they actually have a point-of-view that should be part of the public debate. One way to think about organizing Congress and select committees and others is to provide this kind of platform for those voices. In regard to the Iraq war and other things, there were very intelligent analyses being made that were not part of a strong debate within the administration.

That would be a way to think about Congress's role, even though Congress itself does not have the information it would need to be an effective collocutor.

Walter Pincus (*from the audience*):

This is based on experience. Congress is a body of 435 house members and 100 senators. I happened to work for Senator Fulbright, who was resourceful as hell in getting information when he wanted it. There are a whole bunch of examples.

I investigated the U.S. military abroad, including in Laos. Instead of calling the assistant secretary for Asian affairs to testify, we brought the military air attaché back from Laos, who had discussed the bombing with me in Laos, and made him testify. He laid it out on the record for the senators, rather than just hav-

ing me do a report and having the senators ask questions of the assistant secretary.

We also looked into the nuclear weapons issue. I thought that putting U.S. nuclear weapons into a foreign country was a commitment that surpassed even treaties. So as part of a survey around the world, I went into every country where there were nuclear weapons and asked what the agreement was that brought them in, what the agreement was to use them, and what the agreement was to take them out. It turned out that nobody had ever developed that series of questions before. There were even two countries that did not know we had the weapons there. When we asked to have testimony before the Foreign Relations Committee, the Nixon administration's answer was that the Joint Committee on Atomic Energy was the only committee that could receive the information. Fulbright did not like that.

The Spanish base agreement was up at the time. David Packard, the Deputy Secretary of Defense then, came up to testify in closed session. In the midst of the testimony, Fulbright asked whether we had nuclear weapons in Spain. Packard said that he did not know. Fulbright said that he wanted to know, and Packard said that he would find out.

"No. This is a closed hearing," Fulbright said. "We will empty the room. Call up and find out." So we left the room and he called. He then came back and testified about what happened. Fulbright, that evening, wrote a letter to the Secretary of State saying, "The Deputy Secretary of Defense can get this information on an unsecured telephone call, and you tell me that you cannot testify about it. Therefore you have no power in the government, and we will withhold your financing until you come through." A week later they had a briefing.

So there is enormous power, but you need a member who wants to use the power he has, and it is a political power. It has nothing to do with statutes, the Constitution, or whatever.

Prof. Richard Pildes:

If I can just press this point, those are examples of divided government. Also, there is no question that when you have a long war that has become very unpopular and the president's popularity is very low, then even members of his own party will start piling on to some extent.

Regarding Stephen Holmes's point about the desire to develop sensible policies in an ongoing way, in the novel situation responding to modern terrorism, you want this input upfront. Can you get it? Can Congress play a productive role without the opposition party being given these kinds of powers? Or are these powers in the hands of the opposition party just too dangerous? Would it create just too much partisan conflict?

Prof. Jack Goldsmith:

I think that in that situation only an enlightened president can force Congress to do it, and enlightened presidents have done so in the past.

Barton Gellman:

Even in a very empowered and aggressive Congress, its interests do not necessarily coincide with a full public debate about the truth. Congress also is made up of people and parties with political interests. In the case of a popular war or a popular policy – or a policy they think would be risky for them to talk about, just as much as it is for the president – it will not be talked about. Critics will not have the basic information they need in order to challenge the policy and to provoke a public debate which could change it.

Scott Horton (*from the audience*):

The discussion we are having again comes back to a focus on Congress and Congress's role. This really is key. I think this is essential to it. Stephen Holmes talked about Max Weber's study on this. One of Weber's points that Stephen did not talk about is the institutional game that was played. He saw secrecy being

invoked and used to empower one institution over others, but the focus there really was the parliament.

He said that the bureaucracy and the general staff used state secrets during the war to cripple parliament, to make it a complete irrelevancy and effectively to establish a military dictatorship in the country. That is a powerful example. The U.S. historical record shows that Congress has exercised effective control and restraint over state secrets, and contributed to an important improvement of the public dialogue on these essential issues, especially in regard to war.

Question (*from the audience*):

What is the current law, as far as keeping documents forever secret? Can the U.S. government do that?

Barton Gellman:

There are actually many laws and executive orders pertaining to this. There is a 30-year review process. The president in this administration has asserted the power to stop public disclosure, even if the former president, whose papers are at issue, is willing to disclose them. Certainly, the current executive may choose not to release information and can also prevent others from releasing it.

That is where we get into the whole set of restraints on disclosure by current or former employees. Jack Goldsmith has written a book that I would dearly like to read. I fear that either it will be a very long time before I can read it or big chunks of it will not be there, or both, because the government has exercised much more aggressive and politicized pre-publication review.

The War on Terror and the Courts

Panelists:

Elaine Cassel, Joshua Dratel, Anthony Lewis, Adam Liptak

Moderator:

Prof. Burt Neuborne



Anthony Lewis. Photo by Dan Creighton.

Prof. Burt Neuborne:

In discussing secrecy in the courts, we are talking about decisions regarding not only actual secrecy but also what kind of forums we have. We have at least four forum choices in which we could prosecute national security cases. They can be prosecuted in Article III courts with the ordinary rules that govern the prosecution of organized crime cases, which often involve very sensitive pieces of data. We could build a whole new Article I court system to deal with terrorism issues, similar to what many other cultures have done. We could use the traditional military system, or we could do what we as a people have done thus far, which is to create an institution of maximum secrecy. In preparing for this panel, we discussed whether that system of maximum secrecy falls within the scope of the panel – the war on terror and

the courts. We decided that we would have to amend the title of the panel to “The War on Terrorism and the Courts and Court-like Institutions.”

Adam Liptak:

I have been thinking about what it is that distinguishes the post-9/11 judicial decisions and tactics on secrecy. Courts, of course, have had to determine how to handle secret information for some time. The conclusion that I have come to, reluctantly, is that what we have seen is a version of the administration’s argument best articulated by John Yoo, which is a totalist argument, a showstopper of an argument. In the Yoo conception of the commander-in-chief power, what the commander in chief says, goes. I do not make that point in order to mock it. There are situations in which that conception must be true and other situations in which it may be true. But in the judicial setting it is difficult to reconcile the idea that the administration’s assertions of secrecy must be accepted without further argument with a conventional understanding of how litigation is conducted – in the open and by adversaries. That adversarial structure is central to the conventional understanding of how the American judicial system works.

I have a pair of quotes from pre-9/11 cases in which people whom you would not necessarily think would be sympathetic to this point make it fairly strongly. Justice Felix Frankfurter, in *McNabb v. United States*, said that “[t]he history of liberty has largely been the history of the observance of procedural safeguards,” of the ability to make sure that arguments are made, heard, addressed, and engaged. Judge Frank Easterbrook, now the chief judge of the Seventh Circuit, said in *Union Oil Co. of California v. Leavell*, “Judges deliberate in private but issue public decisions after public arguments based on public records. . . . Any step that withdraws

an element of the judicial process from public view makes the ensuing decision look more like fiat”

But we are going to talk about enormous aspects of the judicial system that have been withdrawn from public view. The judges of course are complicit in this. In 1986, in an access case brought by *The Washington Post*, the Fourth Circuit, of all courts, said:

... troubled as we are by the risk that the disclosure of classified information could endanger the lives of both Americans and their foreign informants, we are equally troubled by the notion that the judiciary should abdicate its decisionmaking responsibility to the executive branch whenever national security concerns are present. History teaches us how easily the specter of a threat to “national security” may be used to justify a wide variety of repressive government actions.

But more recently, in March 2007, the Fourth Circuit ruled on the claims for tort damages brought by Khaled el-Masri, a German citizen mistakenly kidnapped and then abused by the CIA. The court, practically acknowledging the merits, held that it could not let the case go forward because it would expose state secrets. Those state secrets might include crimes committed by the state. They might include crimes and torts committed by private contractors. But the court bought the argument that the state secrets privilege, which the administration is very fond of asserting, is an argument-closer, divesting the courts from the ability to hear cases that historically we thought they were entitled to hear.

The “mosaic theory” is another kind of

show-stopper argument that is very hard to combat. The premise is that innocuous-seeming pieces of information cannot be disclosed because the bad guys would fit them together with other pieces of information to create a larger picture. I suppose that may be so, but how do you test that?

Walter Pincus mentioned, quite rightly, that that the *AIPAC* case is very important as a matter of substance. It is important as a matter of procedure, too. The government is prosecuting people under the Espionage Act and yet it wants to close great portions of the trial. So we now see the government using secrecy not only as a shield but also as a sword.

I am not going to discuss the Guantanamo tribunals because there are others on this panel who are more expert on the topic than me, and who have first-hand knowledge of what goes on there. But those tribunals are a moving target. It is such a “make the rules up as we go along” setting that is hard to see those court-like institutions as legitimate. There is an additional kind of moving target that the administration seems to employ. When a case presenting terrorism-

related issues seems to be on the cusp of being decided the rules of the game are suddenly changed – Yaser Hamdi was released, for example, and Jose Padilla was transferred into the Article III criminal justice system. The best example is that just as the case regarding the National

Security Agency’s surveillance program was to be argued in the Sixth Circuit, the government essentially said, “Not to worry, we have solved the problem.” How did they solve the problem? As best as one can determine, a judge – whose name we still do not know, in the secret Foreign Intelligence Surveillance Court, in a nonadversarial proceeding that cannot be appealed – decided something. Nobody knows what that



**“Enormous aspects
of the judicial system...
have been withdrawn from
public view.”**

Adam Liptak

something is. Yet on that basis the challenge to the constitutionality of the NSA surveillance program is meant to go away. Again, the argument is a show-stopper.

Partly because it was so Kafkaesque and amusing, I want to talk just for a moment about the government's attempts, for which I do not know a precedent, to reclaim secrets that had already gone out. When I used to practice media law, an attorney could say "Judge, the horse is out of the barn," and the judge would know what you meant. The government has subpoenaed the ACLU for a document that had been provided to it. In the end, the document turned out not to be very interesting. It was about the circumstances in which prisoners of war can be photographed. The ACLU got the document, did not think very much of it, and did not do anything with it. But, lo and behold, they receive a subpoena. The subpoena would perhaps have been legitimate if the government were seeking a copy, or even seeking the original and allowing the ACLU to keep a copy. But this subpoena sought *any and all* copies. This was an attempt to reach out, reclaim, and erase from the historical record every version of that document.

In an Oregon case, an Islamic charity, the Al-Haramain Islamic Foundation, has argued that it was mistakenly given what it says is a transcript proving that it has been surveilled by the NSA. Consequently, they argue (and this sounds right to me), they do not have a problem regarding their standing to sue. If the NSA's surveillance caused injury, they specifically suffered it. The government's response was to try to reclaim every copy of that transcript. When federal judge Garr M. King confronted the government lawyer about their mode of argument,



“I have been involved in a number of cases that entailed either classified information or other secrecy issues. The questions are multifaceted and not always about access, particularly public access.”

Joshua Dratel

because the transcript had gone out all over the world (including to journalists), the lawyer replied, "It's secret from anyone who has not seen it. The document must be completely removed from the case and the plaintiffs are not allowed to rely on it to prove their claims." Judge King's response (which I quite like, because he was trying to be sympathetic in a way and I think he put his finger on it) was, "My

problem with your statement is that you assume you are absolutely correct in everything you are stating, and I am not sure that you are."

The theme that I have tried to run through these examples is that, at least in the judicial setting, it cannot be that one party is allowed to say "I win" before the other party can engage its arguments or the independent decisionmaker can hear, digest, understand, and rule. Yet, over and over again, we see the administration making these sort of totalist claims.

Joshua Dratel:

The perspective of defense attorneys like me is fundamentally different from that of journalists and others. The public's right to know is essentially a secondary interest for us because our obligations to our clients, and our interest in securing justice and fair trials for them, are paramount. We cannot let the public interest override those priorities. We always have to keep that in mind in cases that have implications beyond just the individual or individuals on trial.

Prosecutors have the same interests. There is often tension between prosecutors and other government branches or agencies as to what information should, can, or must be disclosed (even with a court order) to a defendant or

defense counsel in cases that have national security implications. That tension can often be exploited by the defense, although not as frequently as in other types of cases. With internal spy cases, for example, someone working for the FBI or the CIA and being prosecuted for espionage has the ability to say, "There are secrets that I will reveal in the course of my defense that may compromise other operations." The government must then decide whether to discontinue the prosecution or divulge that information. Often, they choose the former.

More recently, the context has been terrorism prosecutions. The principle issue we face as defense counsel in these cases is that we are precluded from certain information, even with security clearances. My security clearance is no less than the prosecutors', yet we are precluded from certain information by procedural rules and by a culture of secrecy that excludes us. There is an additional level of preclusion, which is classified information that we cannot share with our clients who do not have clearances. Noncitizens cannot get a security clearance, nor can citizens charged in terrorism cases. That has a significant impact.

Secrecy in the criminal justice system is not always a bad thing. For defendants and others, secrecy sometimes vindicates personal and privacy interests that have nothing to do with government interests. Unindicted co-conspirators are not named in indictments and lists of co-conspirators are sealed. The purpose is to protect the rights of people who do not have the ability to come into court and reclaim their good name. The fruits of wiretaps, individual conversations that are not put in evidence, and all manner of discovery are generally off-limits, for good reason.

I have had the pleasure not only of reading Adam Liptak's work in *The New York Times* but also of seeing him at work as a lawyer. In a case in which the judge sealed the jury selection, Adam appeared on behalf of the *Times*. The judge in that case compromised, permitting cer-

tain information to remain sealed while the process was ongoing and to be unsealed at the end. Frankly, from the defense point of view, sealing it was not a bad thing because it limited the amount of extraneous information that could have had an impact on jury selection and jurors' attitudes. The jury was anonymous throughout the trial, which is another impregnable and difficult aspect of secrecy in these cases. You can imagine what it would be like for a juror to be anonymous and what that would tell him about the nature of the case and the nature of the defendants. Regardless of what other excuses a judge might give to the jurors, they can see very quickly why they are anonymous.

My viewpoint has evolved over time. I have been involved in a number of cases that entailed either classified information or other secrecy issues. The questions are multifaceted and not always about access, particularly public access. Even though the issues involve individual cases and individual clients, we as defense counsel are not immune from considering the broader impact despite the fact that we are not permitted to act upon it. There is much information that we are not permitted to share or divulge that could have an impact on a public debate or national policy. I do not have the same rights as journalists. When journalists get the information, the cat is out of the bag. When I receive it, it is still embargoed for all time. After 9/11, I have read information in books and magazines that had been classified in pre-9/11 cases and that I had not been able to share with my clients. The information has never been declassified, although it has now been divulged to journalists and authors. That is a bitter irony.

Secrets in the context of national security litigation can be divided into three categories. The first is genuine secrets, secrets for which one can appreciate the need for secrecy, including sources and methods. These secrets should not affect litigation because, as I said, I have a security clearance equal to the prosecutors'.

Sharing the information with the defense counsel so that he could make arguments and defend his client does not compromise national security. The proceedings are sealed. There is a federal statute, the Classified Information Procedures Act (or “CIPA”), that governs the use of classified information in these proceedings, and it is very effective. The statute may be unconstitutional. I have argued that it is unconstitutional in certain respects. But even if I were to concede its constitutionality, there is no reason to prevent defense lawyers from participating in the process.

The second category is tactical secrets – those in which the government uses its secrecy powers to decide what to declassify, what should remain classified, and what not to share. There is something called “Section 4” of CIPA, which permits the government to go to the judge *ex parte* and say, “We do not think we should share this.” The defense cannot argue otherwise. I am sorry that I cannot give you examples, but I know from subsequent disclosure that some of the bases for keeping information secret have been invalid. I could have proven them to be invalid if I had been given the opportunity to argue at the time. You unfortunately hear about these things two or three years later, after your client has been convicted and is serving a life sentence. Whether or not to use Section 4 is a case-by-case decision by prosecutors. Some districts and some prosecutors use it more than others. You can see the difference when you litigate several of these cases.

The third category is political secrets – those that have a broader impact and for which the decisionmakers are not the prosecutors but rather people in other government agencies. These political secrets are either too embarrassing or too sensitive for the government to reveal, not because of any security interest but because of their political ramifications. Unfortunately, there are only a limited number of examples in the public record that I can point to, but I will try to share a couple that are in

order to give you a sense of the landscape.

The Foreign Intelligence Surveillance Act (or “FISA”) was enacted in 1978 in response to a Supreme Court decision known as the *Keith* case that said the government could not wiretap domestically for national security purposes without a warrant. It created a hybrid warrant; not really a criminal warrant but an intelligence warrant. The secret Foreign Intelligence Surveillance Court, which Adam mentioned, hears all of the warrant applications. The number of applications has boomed in the past five years. On an annual basis, the number of applications is now double what it was pre-9/11. The applications in one year can now surpass the total number of applications from the time the statute was enacted until 1995, when it began to be used more.

The subject of a FISA warrant would not know about the warrant unless he were prosecuted. There is no notice requirement, as there is for ordinary Title III criminal wiretaps. For Title III criminal wiretaps, there is a statutory requirement that everyone overheard must be given notice of that fact within a reasonable time after the wiretap is unwound and the investigation closed. There is no such requirement under FISA. We see only those people who are actually prosecuted, the narrow tip of the iceberg. There are two provisions in the statute that permit the court to release the underlying affidavits and orders to defense counsel for due process reasons or to assist the court as a fact-finder. Not once has that information been released to a defense attorney. The issue cannot be litigated. The government has a perfect record litigating the validity of FISA warrants. In a recent case of mine, the government argued, “Our perfect record shows that all the warrants are valid and supportable.” I replied that a perfect record is inherently suspicious and that I would win every motion too if I could deny my adversary the right to see the facts. This is a pre-trial question addressing the fundamentals of how the government



Prof. Burt Neuborne, Joshua Dratel. *Photo by Dan Creighton.*

collected the evidence.

The government also has the ability to either declassify or maintain classification of the underlying interceptions of a FISA wiretap. To its credit, the Southern District of New York, to my knowledge, has never refused or failed to declassify a FISA wiretap relevant to a specific case, even relevant wiretaps other than of the defendant. Other districts do not follow the same policy. It is not a national policy for national security. It is purely a tactical decision to deny the defense the right to this information.

I can get access to this information. I am involved in a case in which there are more than half a decade of FISA intercepts of many phone lines and multiple defendants. The defendants are not permitted access to those conversations. They are permitted access only to what are called “declassified summaries,” which in this case were declassified two years after the fact. In other words, we got those late. That was the government’s attempt to compromise. Imagine defending a case involving more than five years of your client’s telephone conversations (which occurred more than five years ago). You cannot prepare, you cannot put your client on the stand, but the government gets to declassify those conversations that it wants to put in evidence.

The summaries that we are allowed to share with our client are prepared by language spe-

cialists. They are not the conversations themselves. They are prepared by people who have an extraordinary number of different competence levels. In one case, there was an entire paragraph in the summary about invective, vitriol, anti-Semitic remarks, and all sorts of incriminating language (in a philosophical, not specific, context). When we finally got the conversation pulled out, that language turned out not to exist. The summary was totally misleading for us and even for the government trying to do its job. That is a significant problem.

The ACLU case which Adam mentioned illustrates tactical as well as political secrets (they frequently merge). I represented the ACLU when it received the classified document that the government wanted to subpoena all copies of that had been disseminated. When the government saw that it had a poor position in the litigation and would very likely lose, it did not address the merits. The government instead declassified the document. So that is what you confront. The sword and shield issue that Adam talked about is really just an extraordinary problem. The broader issue is illustrated by the NSA lawsuits. I have been involved in a number of instances in which we were trying to get an answer from the government as to whether a specific defendant or a specific case was implicated by NSA wiretapping. Not once has a judge permitted a defendant even to see the government’s response much less required an answer. In that context, secrecy has a tremendously broad impact on national policy and national debate. Lawyers are very good for that type of inquiry and exposure.

Prof. Burt Neuborne:

One of the points that has emerged from both Adam Liptak’s and Joshua Dratel’s comments is that there must be some sort of systematic strat-

egy going on in which the government moots any case that it could lose. I have seen it in my cases against the government, too. Every time you begin to get close to winning a case, every time a situation in which the traditional indicia of judicial independence and litigation might result in a precedent against the government emerges, you find that the facts have changed and the case is mooted – the cases of Jose Padilla, Yaser Hamdi, and David Hicks are all examples. Either the person is released or transferred from military to civilian custody, or the document is declassified. It happens systematically. I do not think it can be random. There must some self-conscious discipline that is going on that says you litigate as far as you can go, but when it looks like you are going to lose you pull the plug and moot the case.

Elaine Cassel:

I love Adam Liptak’s metaphor of secrecy as a sword and a shield. I think that it has worked both ways in some of the cases I have focused on. The overarching theme that I have seen is that truth is the victim. Whether secrecy is used as a sword or a shield in these cases, we do not get at the truth.

Attorney Lynne Stewart, whom Joshua Dratel is representing on appeal, admittedly violated some Special Administrative Measures (or “SAMs”). I did not learn about them in law school; they did not exist then. The term refers to conditions that the Department of Justice puts upon lawyers whenever they are going to represent terrorist clients. Stewart agreed to certain conditions in order to visit her client in prison, who had already been convicted in connection with the World Trade Center bombings

of 1993. As every law students learns, attorney-client communications are supposed to be secret unless the client waives them. There are some circumstances in which the attorney is supposed to disclose communications but they are rare. In Lynne Stewart’s case, the SAMs allowed the government to listen in on her conversations, confiscate her notes, and read attorney-client mail – all in violation of ethical obligations and the Sixth Amendment.

At some point in time, Stewart surmised that prison meetings with her client were being recorded by the Bureau of Prisons. She made efforts to interfere with the recording and to

keep the conversations between her and her client secret, as they were supposed to be. She did so by, among other things, creating extraneous noise and talking while her client was communicating with the translator. These actions, along with answering press questions about her client, resulted in her being indicted for aiding and abetting terrorism in April 2002. One of the charges was that she answered a question from the press; an answer which the government

argued was a secret message to her client’s followers to commit further acts of terrorism. She was convicted and sentenced to 28 months in prison. The government wanted 30 years and is appealing the sentence. I suspect that the government already has what it wants, though, because she will never practice law again unless her conviction is overturned.

Jesselyn Radack, who was a rising star in the Department of Justice, is another victim in this sword-and-shield metaphor. She was an attorney on duty in the Office of Legal Counsel when the FBI wanted guidance on interrogating



“The lawyers taking these cases are defending not just their clients but also each and every one of us. They are trying to right a justice system that has been derailed through lies and secrecy, and this is a war that we cannot afford to lose.”

Elaine Cassel

John Walker Lindh, whom they had captured and were holding in a refrigerator unit in an Afghanistan prison.

Radack, along with others at the highest level of the FBI and the Department of Justice, knew that Lindh's parents had retained an attorney. The attorney himself had also notified the DOJ and the FBI not to question Lindh without his presence. Over the course of a frantic weekend, Radack exchanged numerous e-mails with the FBI about the limits of questioning consistent with established case law. The FBI ignored her, extracted statements, and attempted to use them in court. When Lindh's attorney, Jim Brosnahan, made motions to have the statements tossed out, he asked the government to turn over evidence of all of the communications concerning the advice that the FBI had been given by the Department of Justice about Lindh's interrogation. Radack found out, quite by a fluke, that her supervisor had only turned over selected e-mails. There were several e-mails between her and the FBI that the Department of Justice wanted kept secret.

She was concerned about the ethics of this and sought legal counsel of her own. She eventually turned over all of her e-mails to the prosecutor in Alexandria, Virginia. (She had to have them restored to her computer because the Department of Justice had purged them). It is believed that the content of the e-mails were, in large measure, responsible for the government giving up its seeking of consecutive life sentences for Lindh and for Lindh agreeing to a 20-year plea deal (which now in light of the *Hicks* case does not look too good).

But Radack's problems were just beginning. Although she had received stellar performance evaluations, she was fired and became the subject of an unspecified criminal investigation. So she lost two jobs when the FBI showed up at her law firms and essentially said, "This young attorney who you have just hired is under investigation. We cannot tell you why or for what." Eventually, the FBI closed its sham investiga-

tion, but John Ashcroft was not finished with her yet. He filed bar complaints in the two jurisdictions where she was licensed, claiming that she had violated client confidences. The client was the U.S. government. She had disclosed to the federal prosecutor (this is bizarre) and the federal judge secrets that the Department of Justice wanted secret. She is now employed, after being unemployed for four years, but I doubt that she will ever recover from the crime of telling the truth to the federal courts.

We have talked about the Jose Padilla case several times this morning. Padilla's lawyers, Donna Newman and Andrew Patel, have fought a battle that is actually going to trial next week. They succeeded in getting their client into an Article III court, but not without a fight. Padilla was arrested on a material witness warrant. His attorney, Donna Newman, filed a motion in the federal court in New York City asking about the investigation. The government basically said, "We cannot tell you what it is, but since you asked, we are going to declare him an enemy combatant, take him out of New York, and send him to the Fourth Circuit where we will not have these pesky New York lawyers bothering us." They, of course, did not tell her that. She did not know for sometime that her client had disappeared.

The criminal case is now going to trial in Miami. They are facing continuing bizarre tactics, including the government's insistence that certain of the witnesses be disguised or hidden behind screens so that they cannot be identified. In the government's view, it is bad enough that they have to testify at all but at least we will not know who they are. So, the idea of secret evidence and secret witnesses continues.

Some lawyers have beaten the odds. We talked earlier about the *Hamdi* case. That case is particularly sad to me because Frank Dunham, who represented Yaser Hamdi in the Supreme Court, was a personal friend of mine. He had given up a lucrative practice to set up

the first Federal Defenders Office in Alexandria, following September 11th. When he read about Hamdi in the newspaper, he said, “Boy, that guy needs a lawyer and I want to represent him.”

Dunham went to the federal judge in Norfolk, where Hamdi, a dual American/Saudi Arabian citizen, was being held. Dunham said to Judge Robert Doumar, “Appoint me. I want to represent him and file a habeas corpus petition. I want to know why he is an enemy combatant.” Over the strenuous objections of the government, Judge Doumar agreed. Dunham convinced Judge Doumar that you cannot hold a man without you saying why he is being held. The judge was incensed that the government would not tell even him. He said, “I have a naked affidavit,” as he called it, “and you are not even telling me, a federal judge, what it is about.”

The *Hamdi* case was overturned in the Fourth Circuit and eventually went to the Supreme Court. It was the last case that Dunham ever argued, because he died of brain cancer in the fall of 2006. Justice O’Connor wrote, thankfully, that the war on terrorism is not a blank check for the president. But within weeks after the Court’s decision, Hamdi was released after agreeing to return to Saudi Arabia. We will never know what secrets the government was hiding. But we are beginning to suspect, as Scott Horton suggested this morning, that many of the secrets in these cases have to do with torture, or at least coercive interrogation tactics.

Frank Dunham, Joshua Dratel, Jameel Jaffer (who will speak later), and many other lawyers are trying these cases, representing individual defendants, enemy combatants, Islamic charities — they have challenged the government’s claim of a secret system of justice. They are, by and large, public defenders or court-appointed counsel. These positions are the legacy of Clarence Gideon, who challenged the Supreme Court to give meaning to the Sixth

Amendment by appointing counsel for people unable to hire their own. Anthony Lewis, who will speak next, wrote eloquently about Clarence Gideon and that watershed case in *Gideon’s Trumpet*. For Gideon, having a lawyer meant the difference between freedom and imprisonment for one simple reason: only when he had a lawyer could the truth about the case and his innocence be presented. He could not have done it otherwise.

In the *Moussaoui* case, Zacarias Moussaoui’s lawyers fought diligently to expose some of the sham secrets, which turned out to be lies. David Hicks, one of the “worst of the worst,” is now on his way back to Australia. What is the secret that the government was hiding? Whatever it was, it was enough that the government did not want the truth to be out.

Several speakers today have talked about the use of secrecy and how it challenges our democracy. Federal judge Damon Keith, in the 2002 case of *Detroit Free Press v. Ashcroft*, said that “Democracies die behind closed doors.” So does the truth and so does justice. The Supreme Court recognized the significance of lawyers as the gatekeepers of justice when, in *Gideon v. Wainwright*, it said that justice would not be done if the constitutional safeguards of the Sixth Amendment were lost. I believe that the cases we have today are far more complex and far more significant even than the case of Clarence Gideon. I would say that the lawyers who are taking these cases are defending not just their clients but also defending each and every one of us. They are trying to right a justice system that has been derailed through lies and secrecy, and I believe this is a war that we cannot afford to lose.

Anthony Lewis:

I would like to thank Elaine Cassel for mentioning Jesselyn Radack (an entirely unknown, underappreciated victim of what we have been hearing about today) and Frank Dunham, whose argument in *Hamdi* was wonderful and passion-

ate. I was very glad to hear them mentioned.

This morning, Walter Pincus said that *The Washington Post* always goes to the government when it gets a story that includes classified material. I do not doubt that is true. Dana Priest confirmed it and I am sure it is true. The reason you can go to the government, and we forget

this, is because of the Pentagon Papers case, *New York Times Co. v. United States*. A British editor who found out a secret would not go to the British government because a few minutes later a judge would enjoin him from printing the story. That does not happen in this country because, through a series of accidents and good luck, the Supreme Court declined to enforce an injunction against *The New York Times* and *The Washington Post* publishing the Pentagon Papers story.

What were the accidents? First of all, the key thing was that *The New York Times* did not go to the government. The reporters studying the material in the Pentagon Papers, the secret history of the origins of the Vietnam War, were confined in a suite of rooms in the Hilton hotel in New York, with armed guards at the door to keep anybody from knowing about it. We kept it secret so that the Nixon administration would not know that we had the story. Hence, the *Times* published three days of that story, with lengthy text, before the case came to court. When it did come to court, the judge, a former Army intelligence operator, was able to see that the government's claims – that the country would fall and North Vietnamese troops would be walking down Broadway if we were allowed to publish this stuff – was a bunch of hogwash. He could read the stories in the newspaper. He saw that it was all history. If it had all been left to speculation, if nothing had been published



“We are being deliberately kept in the dark about an official policy of torture by the United States government. I think it is appalling.”

Anthony Lewis

and the government had been able to come into court and say, “They have top secret material – 44 volumes worth of it. The country is going to be destroyed,” very few judges would have resisted the demand for an injunction, in my opinion.

There was another little stroke of luck that I will just mention. The

government wanted to retrieve the original documents that the *Times* had, which would have disclosed the source. The paper refused to turn them over, and the judge held that the paper had a privilege. He could not hold that way today.

The Supreme Court decided the case by a majority of six to three, with a very distinguished justice, John Harlan, dissenting. He wrote that there has to be a premise that the executive branch prevails. Under Harlan's view – and I have a lot of respect for Justice Harlan – hardly ever would a court have declined that injunction.

So, through a series of circumstances, the law became such that injunctions against publication cannot be issued in most cases (not every case, but most of them). That has made a great difference. That is why Walter, Dana, and others can go with confidence to the government to consult on these matters

But, on the whole, judges are very reluctant to tangle with the executive branch on issues of national security. Not long after the Pentagon Papers case was decided, *United States v. The Progressive, Inc.* came along, in which a judge enjoined *The Progressive* magazine from publishing what it called “The H-Bomb Secret.” That was its cover line. The injunction lasted for months, despite the Pentagon Papers decision. The government had predicted horror and disaster if *The Times* was allowed to continue publishing the Pentagon Papers. But in the

Progressive case a few months later, it basically said, “That was just history. That was not important. This is really important. You have got to stop this.” And the judge did stop it.

Victor Marchetti wanted to publish a book called *The CIA and the Cult of Intelligence*. The CIA censored hundreds of passages in the book. It finally agreed not to insist on some of the deletions, including the fact that CIA director Richard Helms had mispronounced the name of the Malagasy Republic. Imagine how secret that was. Chief Judge Clement Haynsworth, a very good judge in the Fourth Circuit, said in *Alfred A. Knopf, Inc. v. Colby*,

“There is a presumption of regularity in the performance by a public official of his public duty,” at least in the national security area. That was pretty much the dominant view. He went on to say, obviously with reluctance, “The author of this opinion has examined some, but not all, of the 142 deletion items. The information in at least some of them does relate to sensitive intelligence operations and to scientific and technological developments useful, if not vital, to national security.” On that basis, he threw Mr. Marchetti out of court in 1975.

In June 2006, Judge John Gleeson of the Eastern District of New York, in the immigration case of *Turkmen v. Ashcroft*, said that the government’s conduct “was not so irrational or outrageous as to warrant judicial intrusion into an area in which courts have little experience and less expertise.” That is the dominant view. Judges are reluctant to tangle with government decisions on issues of security, or so I think.

I want to return to the very important truth about secrecy and torture mentioned by Scott Horton and Elaine Cassel. Many things have

gone wrong in this country and in its relations with the world in the years since 9/11. To me and my sense of what my country is about, nothing is worse than the fact that the United States government consciously and deliberately practices torture (often by other names, but it amounts to torture). I would be willing to bet that the people like John Yoo who authorized or advocated it would not be very pleased if they were subjected to such conditions themselves.

It has been protected by a deliberate policy of secrecy – that is what we have to keep in mind. Yaser Hamdi has already been mentioned.

He was taken into custody as an enemy combatant and held without charge, without trial, and without access to counsel for years, on the ground that what he knew, what he believed, or what he had done was so dangerous that he could not be allowed to have contact with any other human being. Then, when he won his case in the Supreme Court, the government sent him back to Saudi Arabia rather than having the case

tried. Suddenly this dangerous man was at large. Every effort has been made, successfully so far, to keep anyone from publicly testifying about torture. Many leaks have occurred. Many former detainees have talked to the press or to lawyers about what was done to them. But, in court, none have been allowed to talk publicly about what happened.

Scott mentioned Abd al-Rahim al-Nashiri. When the transcript from his hearing (“trial” is too grand a word for it) was published, every response to the question “What did they do to you then?” was blanked out. It has all been blanked out. We are not allowed to know. Torture underlies a lot of this. I could not agree more with Scott Horton.



**“To ask judges to be heroes
in areas where they
do not have any information
may be asking more than
human beings are
capable of, or legal systems
are capable of.”**

Prof. Burt Neuborne

The judge in Jose Padilla's criminal trial recently made a decision rejecting the claim that the trial should not be allowed to proceed because of improper government behavior during the years that Padilla was held in custody, without charge, as an enemy combatant. But the defense had wanted to have a hearing, had wanted to produce evidence, had wanted Padilla to be able to testify about what was done. That was also denied – not just the substantive decision, but even the right to put on evidence on the subject. We are being deliberately kept in the dark about an official policy of torture by the United States government. I think it is appalling.

We need to care about this. A policy of secrecy that protects abuse of all kinds, torture being the worst, but also many other things – detention without trial, indefinite detention, the detention of the prisoners at Guantanamo Bay (hundreds of them who will have no proceeding at all, who will just be kept there without even rudimentary process to determine whether they should be kept) – all of these things are grist not only for the brilliant journalists who have appeared here today but for all of us as citizens.

Prof. Burt Neuborne:

Anthony Lewis was kind enough not to point out that I am one of the only lawyers to have lost a motion for an injunction in a setting such as he described. I was one of the lawyers in the *Progressive* case. There was a colloquy with the judge before he issued the injunction. The judge turned to the government lawyer and said, "What are the consequences? If we are wrong, what happens if the formula for the H-bomb gets out to the public?"

The government lawyer said, "We could lose Boston. We could lose Chicago." He said to the judge, "You are talking about the potential for millions and millions of lives." The judge turned to my colleague Bruce Ennis and I and said, "What would happen if I ruled the wrong way for a while? If I balance the dangers

here, how can I possibly not grant the injunction? The human agony"

"Agony" is the right word, because Judge Robert Warren, the district judge in Wisconsin who issued the injunction, was an excellent judge who knew the law, who knew the Pentagon Papers, and who had read everything. He said, "You are asking me, as a human being, to be personally responsible for the potential death of millions of people. The balance you are telling me is that I should uphold a parchment barrier." He said, "I cannot do it because I do not know enough."

The panelists have identified the real problem. To ask judges in a time of crisis to overrule statements by the executive that tell them that they are risking horrible things to hundreds of thousands, perhaps millions, of people unless they fall in line behind the government requires a very strong person. Or you have to be lucky enough to have three days of publication so that the judge can see the government is full of baloney.

Perhaps the worst judicial decision in this country's history was to uphold the Japanese concentration camps during the Second World War. The Court upheld them because there was nobody around who could challenge the statements by the military leadership on the West Coast that there was a great threat posed by some sort of fifth column who was going to seriously interfere with the war effort. There was no way to get additional information into the process that would challenge that assertion.

That is really our challenge – to ask judges to be heroes in areas where they do not have any information may be asking more than human beings are capable of, or legal systems are capable of. We have to confront that as a flaw in the system itself, because it is working itself out now. There are judges now who are afraid, who are cowards. They are afraid that it will be their fault if they make the wrong decision and something terrible happens. Like any

other low-level bureaucrat, they are afraid to take that risk. The secrecy is what makes it possible.

Anthony Lewis:

I could not agree with you more, but how do you explain Judge Doumar who, as Elaine Cassel said, told the government in the *Hamdi* case, “You are going to have to tell this guy why you are holding him?”

Prof. Burt Neuborne:

You are exactly right. There are judges who do their jobs, thank goodness. But they are, unfortunately, in the minority.

This is an administration that gives secrecy a bad name. There is just no question about it. They have abused the power of secrecy to do so many terrible things. But is it clear that there is no role for secrecy in this process; that we should be thinking about a sort of standard Article III model, in which the lawyers get all the information and most of it gets out?

Joshua Dratel intimated that he thought there might be some genuine secrets. If there are, how do we keep them? Or is the price of adjudication having to say that we cannot have any genuine secrets, that they are all going to get out?

Adam Liptak:

I would separate two ideas, which I think Joshua suggested. One of them is getting rid of the adversarial process. I also think you can have an adversarial process that respects secrecy but with attorneys on the other side analyzing, questioning, picking apart legal arguments, cross-examining, and looking for holes in factual presentations. That can be done in secret. I do not think that Joshua discloses to the rest of the world what he has learned in litigation. Having done that, you will also be able to have a much more measured analysis of what truly needs to be kept secret.

Joshua Dratel:

The question is not one of government versus public, or defense versus prosecution. It is more layered than that.

Edwin Wilson is a former CIA officer who was prosecuted for doing business with the Libyans by selling arms and other essentially embargoed equipment and information. He has been in jail for almost 25 years. One of his convictions in Texas has been vacated. It turned out that the prosecutors had told the CIA that Wilson said he worked for the agency in a free-lance capacity even after he left, and that was going to be his defense. They told the CIA that the judge wanted an answer as to whether or not that was true. The agency, in an affidavit signed by its counsel, said, “No, he is lying. We have not had contact with him. It was fleeting and we never authorized anything.” Twenty-five years later, it turned out that Wilson was telling the truth. He had, I think, nine different projects he was working on with the agency. The agency lied to its counsel, who submitted a false affidavit; lied to the prosecutor; then lied to the court and lied to the defendant. This went on within the government itself. It is not just a binary system, it has more layers than that. That is what we have to try to get behind. The courts have a real role in digging, and the best way to dig is to have an adversarial system.

Prof. Burt Neuborne:

Elaine, let me ask you a sensitive and difficult question. In my mind, I cannot equate Lynne Stewart with Jesselyn Radack. Radack, as far as I am concerned, was a hero. She did what every good lawyer should do. She upheld the absolute ethics and morality of the legal system. It is a tragedy she was punished for it and people should rally to her defense. Lynne Stewart, if you believe the jury – and they convicted her – did something that strikes at Joshua and Adam’s ability to stand here and say, “We can have an adversarial processes. You just have to trust the lawyers. The lawyers will be made privy to the

information needed to make the system work. They will carry that very heavy responsibility.”

Joshua said a number of times that there are things he wants to say because they are important in the public arena but cannot. He understands that he could not function in his job if he did. Self-discipline inside the bar is absolutely crucial. If the bar cannot carry out that self-discipline, I do not think that we have a hope of building a system that can work. So I just wanted to ask whether you can equate Radack and Stewart.

Elaine Cassel:

No, I do not equate them at all. In the many articles I have written about Lynne Stewart, I have said that I do not approve of her violating the SAMs and then acting surreptitiously to interfere with the recording. I do not see her statement to the press as that grave a breach.

I believe that most lawyers think that it could have risen to the level of a bar complaint and discipline, even of judicial discipline and sanctions, but not terrorism. I think that what happened in the *Stewart* case and the indictment in 2002 was that Attorney General Ashcroft used her as an example, as a shot across the bow. He was telling lawyers, “You better watch it, because you people who represent terrorists are in danger yourself of being called terrorists.”

Many lawyers whom I know in Alexandria risk their livelihood and reputations by representing terrorism defendants, although it has gone on long enough that they now have the respect of the bar. When they first started representing these defendants, the local bar ostracized them. So Radack and Stewart are not at all the same. I think Stewart is a sad example of extreme overcharging for political reasons.

Prof. Burt Neuborne:

That is a fair comment. Remember the effort in January 2007 by Charles Stimson, the deputy assistant secretary of defense for detainee

affairs, to intimidate the lawyers defending people at Guantanamo by threatening to get the lawyers’ other clients to pull their business. We still do not know whether any clients have taken their business away from those big firms as a consequence of the firms having been so terrific in producing lawyers for the people down at Guantanamo. As far as I know, there has been no systematic study of whether some president of a large corporation has pulled business from one of these big firms because of it. But that was clearly the effect that attempt was designed to produce, exactly as you said.

National Security and Intelligence

Panelists:

Frank Anderson, Jameel Jaffer, Judge Kenneth Karas, Prof. Stephen Schulhofer
(Judge Karas's remarks were off the record.)

Moderator:

Dana Priest



Frank Anderson and Dana Priest. *Photo by Dan Creighton.*

Dana Priest:

This panel is titled “National Security and Intelligence,” but I am going to take the prerogative of the chair and change it slightly to “The Future of Secrets.” I would like the panelists to try to step out of their own shoes at the end of their comments, and to offer some suggestions to their adversaries in this contest.

Prof. Stephen Schulhofer:

I would like to start by saying something about the nature of the threat that we are confronting. There has been much discussion about how 9/11 should change the balance of secrecy. But the United States has suffered devastating attacks before. During the Cold War, we faced a very real threat of nuclear attack. People who did not live through that era believe that modern

terrorism is much scarier, but anybody who grew up in the '50's will tell you that the national security need then seemed as strong as it could possibly be. When we finally woke up to the dangers of unchecked power and unlimited secrecy, it was not because people thought that we were not facing a serious threat or that

the danger of worldwide nuclear annihilation was not a big deal. People were still scared but we realized that we had to impose limits because unlimited secrecy was destroying freedom. People also learned that it simply was not necessary. We learned that unlimited secrecy was not even making us safer; rather, it was actually making us more vulnerable.

The threat today is different in some ways. Our enemies are not deterrable in the same way.

The threat comes from smaller numbers of individuals who are more widely scattered and more difficult to identify. So we do need a wider intelligence net and more emphasis on prevention. But the nature of modern terrorism also means that human intelligence sources are crucial. The government must be trusted, not feared, by the people with whom our enemies are living, working, and worshipping. The distinctive features of modern terrorism do not make accountability less important. In fact, they make it more important.

The administration has successfully persuaded much of the American public that oversight of executive powers will somehow render those powers ineffective. The truth is just the reverse. The problem we face is how to figure out when secrecy is justified and when it is not.

One answer, probably the prevalent one

among the public today, is to play it safe. If in doubt, classify. In practice, that means that the executive branch can keep secret, or at least legally try to keep secret, literally anything that it wants to hide. By playing with some version of the mosaic theory, you can construct a plausible scenario in which any revelation of anything will help some terrorist somewhere.

Disclosure always poses some risk but giving the government a free hand to prevent it is risky too. There is no way to play it safe. The officials who control disclosure will sometimes put political or their own career interests ahead of the public interest. That will happen as long as they are human. In my opinion, some secrets should be subject to disclosure even when that could conceivably be damaging, because nondisclosure is also damaging. We will never find a formula for identifying, in advance, the cases in which the benefits of disclosure outweigh the dangers. We cannot articulate a formula for doing that. The focus has to be on designing a good system for making the decision.

The earlier panel chaired by Prof. Richard Pildes aired a number of possibilities. Professor Stephen Holmes suggested an adversarial system within the executive branch. Professor Pildes was pushing for a congressional checking function by the opposition party in a divided government. Professor Jack Goldsmith suggested that it must be within the executive branch and that we just have to hope to have good people there.

We have a pretty good system right here in this room – the reporters who have made the system work by great investigative reporting and careful judgments about what should and should not be reported. It is an informal, ad hoc system with very intangible incentives and checks. From a lawyer's perspective, it looks hopelessly haphazard, but it does work. As Dana Priest said this morning, it has made much information available. But it is not enough. Using Congress, or the opposition

party in Congress, as a check is not enough either. Congress does have great incentives to delve into secrets in the executive branch but it is not always going to have the incentives to look for the right things or to disclose the things that should be disclosed.

We need to have a system of disclosure governed by formal, legally enforceable rights to obtain information. Faith in those sorts of rights is very much out of fashion these days, in law schools at least. It is considered much more sophisticated to admire a system of socially and politically grounded results, such as those that emerge from the relationships between good journalists and their sources. But that is not adequate. It does not take away from the great work that Dana, Walter Pincus, and others have done to say that the results of that process are woefully inadequate.

For one thing, we have not begun to know the famous “unknown unknowns;” the things that we should know but will not for years, if ever. We should talk about the unknowns that we do now know, such as the NSA wiretaps. We have learned about them thanks to some very courageous and creative reporting. There were a few ripples of dismay (confined mostly to lawyers) but, of course, the wiretapping continues. Some people say that the administration has backed down on the wiretaps. But has it? We do not really know. The Senate would like to know, among other things, if they have really changed what they are doing. But the administration says that the specifics must remain secret. If James Risen (who broke the story) knows the answer, his editors may make him wait until after the next election to publish it, like they did the last time. So we will not really know.

The important thing is that the wiretaps will not stop, whether they are illegal or not. In spite of the very constructive debate that these kinds of stories trigger, they will not stop until the Senate can compel disclosure of the facts or the pending lawsuit produces a definitive ruling.

But Senate subpoenas and lawsuits cannot succeed unless there is a legal right to overcome the administration's claim of state secrets privilege.

One theme that Professor Burt Neuborne raised a few minutes ago potentially colors the issue. He focused on the need to get judges tuned into a culture of skepticism about these claims. I very much agree but we are not there yet. Outside of criminal cases, the government has the state secrets privilege as a trump. Judges do not even begin to get into the process of balancing.

The same problem exists regarding the CIA black sites. We now know about them, thanks to Dana. There has been a tremendously valuable debate. Europeans are investigating, and some of the sites have been shut down or at least relocated. But, again, there is no real leverage. Unless a legal forum is available, there is not even a definitive way to refute the disingenuous denials and evasions that come from the administration. So far, every lawsuit challenging these practices has been dismissed on grounds of something like the state secrets privilege. Legal rights without good journalism would not be worth much. That is not what I am suggesting. But good journalism without legal rights does not have nearly enough traction.

In order to make progress, we have to have strong ways of getting information as a matter of legal right. Even though we cannot define the scope of that right in the abstract, we can use the Classified Information Procedures Act, which Joshua Dratel mentioned, as a model. That is the framework that lets judges in criminal cases assess the need for secrecy and then craft unclassified equivalents for the classified information or penalize the government in an



“The administration has persuaded much of the American public that oversight of executive powers will render those powers ineffective. The truth is just the reverse.”

Prof. Stephen Schulhofer

appropriate way if it insists on withholding the information. In civil cases – alleging torture or rendition, for example – there is no equivalent. The claim of state secrets privilege gives the government a magic wand that just makes every inconvenient lawsuit disappear.

Freedom of Information Act requests and congressional subpoenas face a similar obstacle

course. We need a CIPA-like system that would mediate these secrecy dilemmas in a very fine-grained, case-by-case way, so that we would have something other than a haphazard check on self-serving secrecy claims by the executive branch.

There are two problems with what I have just suggested. First, how do we know that federal judges using CIPA-type powers would not defer too much to the government? We do not know. In fact, we can be pretty sure that they would. The CIPA disputes in the *Moussaoui* case and several of the others mentioned earlier are clear examples of judges deferring too much. CIPA is not a cure-all. If we took the step of moving that system into the civil courts, it would then be ripe to address the problem that Prof. Neuborne raised about having it function in an appropriate culture. But first we have to put it in place.

Although CIPA is not a cure-all, it absolutely guarantees that the underlying facts will at least be disclosed to a fully independent judge and that the decisions about secrecy, whether too deferential or not, will be made by a judge rather than the executive branch. In our system, that is as good as it can get.

The second problem is the mirror image of the first – the competency of a federal judge to make tricky decisions about the national securi-

ty implications of disclosure. It is a fair point. A judge is not an expert in national security, but there is no evidence that they will not defer heavily to any truly plausible claims from national security experts. More basically, what is the alternative? Judges are not experts in national security but military officers and national security analysts are not experts in First Amendment concerns. I have not seen a mountain of evidence suggesting that national security experts defer heavily to First Amendment concerns in deciding what to classify.

Somebody has to make these decisions. If we want to have a healthy democracy – or a competent, well-functioning national security effort – we have to formally, legally give these decisions to a disinterested, independent institution.

Jameel Jaffer:

I come to these issues from a different perspective than most of the other participants in today's conference, because for the last five years I've been litigating challenges to government secrecy – challenges brought under the First Amendment and the Freedom of Information Act. Given that I am an ACLU lawyer, I guess it is no surprise that I believe that the secrecy surrounding government intelligence gathering is excessive and even dangerous. In my view, the government routinely overstates the need for secrecy and understates the costs, and the institutions that should be serving as checks against that kind of abuse are not playing the role they should be playing. This is not *less* true, but *especially* true, in the context of intelligence gathering.

I am going to focus on just one example – national security letters (or “NSLs”), which you have heard a little about already today. Our experience with national security letters should teach us much about government secrecy and why we should be skeptical of it.

Basically, a national security letter is a demand for information, issued unilaterally by the FBI. The FBI serves them on banks, credit

reporting companies, Internet service providers, and in some cases libraries and universities. Anyone who receives one of these demands gets a gag order along with it – a nondisclosure order preventing them from telling anyone that they have been served with a national security letter. They cannot even say that the FBI has sought or obtained information from them. These national security letters, I think it is widely agreed, are very valuable intelligence tools for the FBI. Even before the Patriot Act, the FBI issued thousands of them every year.

NSLs are often compared to subpoenas but I want to emphasize the gag orders, which generally do not come with grand jury subpoenas. Ordinarily, the recipient of a grand jury subpoena is free to hold a conference to disclose to the world that they received it. The same is not true of NSLs. Consequently, the only possible source of information about national security letters and the FBI's use of them is the FBI itself. With subpoenas, you can get some information from the people who have been served. With NSLs, you cannot.

Soon after the Patriot Act was enacted by Congress, the ACLU filed a Freedom of Information Act request in an effort to get more information about how national security letters were being used. We wanted to know, for example, how many had been issued and to what extent they were being used to seek information about people who were two, three, or four steps removed from the actual target of an investigation. We wanted to know how many times national security letters had been used to seek information about U.S. persons – U.S. citizens and permanent residents. The FBI said that the information was properly classified and that disclosure would jeopardize national security.

You might ask, as we did, how disclosure of that information would jeopardize national security. It would have been different had we been asking for information about particular surveillance targets or particular surveillance investigations. We were not asking for that kind

of information. We had asked only for policy information and general aggregate, statistical data at the policy level that would allow people to understand a little more about the implications of the Patriot Act.

The FBI came back with the mosaic argument. They argued, “This information may seem innocuous on its face, but our enemies have the ability to piece it together with other seemingly innocuous information. By combining this data, they can actually put together something that is very useful to them and that may in the end constitute an extremely significant threat to us. We cannot anticipate in advance which information will be meaningful to our enemies and for that reason we have to withhold any information that might be meaningful.” This argument has found quite a bit of traction in federal court.

The D.C. Circuit Court of Appeals relied on the mosaic argument in rejecting a FOIA request for the names of immigration detainees after 9/11. The Third Circuit relied on it to deny press access to immigration hearings. Many courts have accepted this argument. One consequence is that FOIA litigants are now commonly put in the position of having to convince the federal judge that the information they are asking for is meaningless (since only if the information is meaningless do they have a right to it). The word “Kafkaesque” has been used many times today but this surely qualifies.

We should give the mosaic argument its due. I do not think that it is entirely ridiculous. It may well be true that we do not know which disclosures could aid the enemy. It may well be true that we do not know which disclosures our enemies would find meaningful, but we should be honest about what the consequence would be if the argument were credited on a broad scale. I think that what it would mean, in the words of the Sixth Circuit in the 2002 case *Detroit Free Press v. Ashcroft*, is that the executive branch could “operate in virtual secrecy in all matters dealing, even remotely, with ‘national security’ ...” I do not think that is an overstatement at all.

This kind of secrecy subverts the processes and the institutions that ordinarily serve as safeguards against abuse.

We now know much more about national security letters. In November 2005, Bart Gellman reported in *The Washington Post* that the FBI was issuing at least 30,000 of them every year. In March 2007, the Justice Department’s inspector general revealed that the number is closer to 50,000 a year – that is 143,000 national security letters issued between 2003 and 2005.

The inspector general also revealed that the FBI was systematically violating the national security letter statute by issuing NSLs that were unconnected to any ongoing investigation and by using what the FBI was calling “exigent letters,” which were not NSLs at all but rather freeform demands for information that were not authorized by any federal statute.

It is difficult to believe that we would be where we are now if the FBI had been required to account for its use of national security letters. We are where we are because the FBI was permitted to operate without meaningful oversight. The inspector general’s report disclosed exactly the same statistical information that the ACLU and other organizations sought five years ago, the same information that the FBI had withheld on national security grounds. I have not heard anyone suggest that the disclosure of the information in that report jeopardized national security. Virtually everyone, except the FBI itself, is wishing that the information had come out earlier. There is still much that we do not know about national security letters. That is chiefly a consequence of the gag provisions.

Everybody agrees that some degree of secrecy is going to be necessary in some national security investigations – that is the easy part. But, until very recently, every single NSL came with a permanent gag order. Congress amended the law so that people who receive gag orders can challenge them in court but the amendment is almost meaningless. Under the statute, judges

are required to defer to FBI certification that national security requires secrecy. In many cases, they are required to treat the FBI's determination that secrecy is necessary as "conclusive." That is not deference so much as rubber-stamping what the FBI says is necessary.

At what point does this kind of secrecy undermine the democracy that it is ostensibly meant to protect? I think it is important to recognize that when we are

talking about secrecy we are talking not only about the distribution of information but also about the distribution of power in our society. When we allow information to concentrate or to accumulate in the executive branch, or anywhere, we are allowing power to concentrate there as well. The consequence of that kind of accumulation of power in one place is to deny the public the information it needs in order to evaluate the decisions of political leaders, to hold them accountable, and to pressure them to change policies.

I have focused on the NSL provision but I could have used any number of examples. In many contexts, citizens do not know what the government's policies are. Until *The New York Times* published a story, nobody knew that the government was engaged in warrantless wire-tapping inside the U.S. Until *The Washington Post* published the story, nobody knew that the Office of Legal Counsel had effectively authorized torture. In the intelligence context, especially, secrecy has been used again and again not to protect legitimate security interests but rather to insulate controversial policies – and in many cases unlawful policies – from the processes and institutions that ordinarily serve as safeguards against abuse.

Frank Anderson:

This morning, Dana said something that I have been thinking about throughout the day, and it is an important point. She said, "In the end, this is a contest." In her case, I think that it is a contest between the press and its consumers seeking to know, and the government and everyone else seeking to conceal. Our system is a whole pile of contests. Our system of justice is a contest.

Our system of citizen involvement, government, and the press is a contest. The contest only works when everyone recognizes that there are roles and that there are rules.

The contests are swirling. Journalists and spies live in a similar swirl. We live in this swirl whenever we seek information. We go to a possessor of that information and try to

persuade him or her that their responsibility to keep the secret, and the rules which apply to it, are trumped by some more important rules.

Sometimes, as spies and journalists, we do tell the truth about this "higher" rule. Sometimes we don't. Sometimes we ourselves are influenced by other contests. Spies do not get promoted based on failure to find secrets. Journalists do not get promoted based on telling their editors, "I looked at the Department of Interior, and the Park Service is doing just fine today." Sometimes those rules and roles become distorted by the things that distort all of our lives. They can be distorted by fear and anger. I believe that fear and anger are the greatest distortion.

I have recently found myself briefly switching sides and roles. I have acted for the defense in terrorism cases a couple of times, including one in which Joshua Dratel was involved. I think that I continue to play by the rules that governed my roles over the past three-plus



“When we allow information to concentrate or to accumulate in the executive branch, or anywhere, we are allowing power to concentrate there as well.”

Jameel Jaffer

decades. I have no trouble with this temporary change of roles because the rule I was following was the Constitution. Its defense was more important than an individual's particular defense. I also apply a rule a new personal rule in deciding whether I will play a defense role in one of these trials. I will only participate for the defense if I am persuaded that the person involved is innocent, not just acquittable.

That has been a learning experience. The conclusion I drew from it is that we, as a society, including the Department of Justice, are now acting too much under the influence of fear and anger. We have allowed fear and anger to distort our roles and rules. I think that the pendulum is beginning to swing back, and I am confident that it will.

Incompetence is another problem that gets in the way of playing out roles according to the rules in this game. We are, sadly, incompetent to play many of the roles we are attempting to play. In some of the terrorism cases our government has attempted to prosecute, we do not understand even the language that the people are speaking, as Joshua mentioned.

We are working on the basis of documents that have been either mistakenly or maybe even maliciously mistranslated by government witnesses and experts.

We as a society are arguing even about who the enemy is in the war on terrorism. Some of us have dreamed up a thing called "Islamofascism." (I have no respect for fascism and no great expertise in Islam, but I can tell you it that is impossible to put those two things together without creating an oxymoron.) Yet there are politicians and pundits who want to tell us that this so-called Islamofascism is a

force equal to the threat that was posed by National Socialism or Scientific Socialism, and that we are in such danger now that removing ourselves from Iraq would be like abandoning Britain in 1942. We are collectively acting under such fear and anger that it has affected our competence in every aspect of our lives. To see it distorting our system of justice is particularly disturbing.

The pendulum will swing back. Until it does, as you go out into this swirl of contests, ask yourself every day whether you are playing the appropriate role, whether you are playing according to the rules, and whether you have developed the necessary competence. Are you overcoming fear, anger, greed, and ambition in

order to play properly? If you ask yourself those questions, it will all work out.

Dana Priest:

I would like to ask you a question, since you are the only person on this panel who has had extensive intelligence community experience, even though I know that you are not at the CIA anymore. You mentioned that the pendulum might be swinging. We have talked about contests

and the risks of unveiling secrets. How do you think that might be playing out within the CIA, for example? Are they hunkering down? Are they re-examining and being introspective?

Frank Anderson:

I have no knowledge. Nevertheless, I will pontificate.

Two things are coming out. One is that if there is a global war on terrorism, we are doing very well. We find real cases, not just rinky-dink cases, to prosecute. Frankly, I do not share



“We are collectively acting under such fear and anger that it has affected our competence in every aspect of our lives. To see it distorting our system of justice is particularly disturbing.”

Frank Anderson

the fear. The ideology that we fear has failed in every country where those who follow it have sought to gain power. Islamic extremism, if you want to call it that, has contested for power and lost in countries far weaker than our own. They lost in Syria. They lost in Algeria. They are losing in Pakistan and they are losing in Saudi Arabia. We are not confronted with the Nazi hordes, the hordes of Stalin, or even the hordes of Genghis Khan surrounding Vienna – we are not in that kind of danger. We are contending with people who are struggling in Helmand Province.

There is obviously some very good work being done by the CIA. I only have anecdotal evidence saying that there are things getting in the way – that the bureaucracy is becoming sclerotic, that people are risk-averse, and that it is difficult to be an operations officer in the mountains of Afghanistan if you are only there

for 90 days. I have yet to hear a single complaint from an operations officer saying, “I am unable to do my job because Dana Priest, Walter Pincus, and James Risen are discovering things that we need to keep secret.”

Karen J. Greenberg:

I thought this morning about the scene in *The Wizard of Oz* when the Wizard says to Dorothy, “Pay no attention to that man behind the curtain.” There is a sense that we are not listening or paying attention. The reason we may not be listening is not because we are selfish, stupid, or incompetent but rather because knowledge brings certain responsibilities. Knowing is scary and sometimes we just do not want to know.

One lesson that we can take away from today’s conference is that knowing isn’t so bad. Not until we know can we really start a conversation.

Afterword

Prof. Norman Dorsen

The Center on Law and Security kindly invited me to comment briefly on the transcript of its memorable conference on Secrecy and Government. This is perhaps because I have been involved in these issues since 1954, when I participated as a young lawyer fighting McCarthyism during the Army-McCarthy Hearings and also appeared in the Pentagon Papers case, the Nixon tapes case, and other milestone controversies.

It is a well-known adage that the more things change the more they stay the same. This is certainly true with respect to the ongoing struggle between government’s desire to mask its activities and the public’s need for open government. The perennial conflict existed before the formation of the United States, when the delegates to the Constitutional Convention

voted to bar the public from its deliberations. Nevertheless, I suggest that there should be an asterisk after the longstanding adage in order to take account of the special circumstances in which we live.

Some general propositions seem to me to be timeless. That knowledge is power is perhaps the most important, as several speakers at the conference emphasized, alluding to James Madison’s famous dictum. Another reliable fact is that the executive branch will always, or almost always, seek to protect information, a fact that is reinforced by the petty tyrannies and insecurities of the bureaucracy. A final general proposition that has held true over a long period of time is that judges are reluctant to buck the government on secrecy issues, often saying that they are not “experts” on national security, even though they are sup-

posed to be experts on the First Amendment.

At the operational level, too, the issues are similar over time – for example, whether or not certain documents can properly be classified; whether it is lawful for the government to engage in wiretapping or other surveillance (and the flip side of this question, what must be kept from the public as “state secrets,” an issue being litigated in a Washington federal court as I write); and whether there is an applicable executive privilege going beyond classification and what that privilege may cover.

This leads me to other propositions. The first is that in these areas politics will usually outweigh law in public opinion. Executive privilege provides an example. Charles Wilson, then the secretary of defense, invoked this privilege during the Army-McCarthy hearings to prevent Senator Joseph McCarthy from obtaining information from military “security courts” that Senator McCarthy alleged were departing from the law. Wilson was putting another nail in McCarthy’s coffin on behalf of the Eisenhower administration, and the public – especially the liberal public – cheered because of its antipathy towards McCarthy. But when President Nixon invoked executive privilege to shield his activities from the special prosecutor during Watergate, the public acclaimed the Supreme Court for rejecting it. There were differences in the two situations, but except for a few aficionados of presidential prerogatives this was an irrelevancy in the effort to unseat Nixon.

A second proposition is the importance of a free press. Unfortunately, the press’s performance over the years has been mixed. As early as the reaction to the Alien and Sedition Acts, enacted in 1798, journalists have bravely confronted political authorities, capsulated in the phrase “speaking truth to power.” But during the McCarthy period, apart from a few notable

exceptions, the nation’s newspapers rushed to print Senator McCarthy’s unfounded allegations of Communism in government, including in its secret laboratories. In the run-up to our invasion of Iraq in 2003, most of the press accepted uncritically the assertions of the Bush administration regarding weapons of mass destruction, Saddam Hussein’s link to 9/11, and the rest. The country badly needs a free and courageous press.

At an earlier conference on secrecy and government, held in 1973, Daniel Ellsberg asked, “Where do you draw the line [between national security needs and an open society], and who should draw it?” Ellsberg had earlier handed over a mammoth government survey of the origins of the Vietnam War to *The New York Times* and *The Washington Post*, thus precipitating the Pentagon Papers case and eventually the Watergate crisis. He concluded that the “line should not be drawn only by executive officials who are thus allowed to determine entirely by themselves what the public shall know about how they are doing their job.”¹

The current period has some special features, which I have referred to as an asterisk. The first is that we live in the aftermath 9/11, that is, of major violence against the people of the United States on its own territory – an act that had and continues to have the powerful, and for a while almost limitless, capacity to insulate the executive branch from oversight by the press or the courts and even from major dissent. In this context, every attempt to crack open the fortress of secrecy has had to confront a strong presumption in favor of government policy.

A second element these days is the sweeping nature of the civil liberties violations: confining suspects without providing them with access to a lawyer, or even acknowledging that the person is being held; the use or intended use

¹ NONE OF YOUR BUSINESS: GOVERNMENT SECRECY IN AMERICA, 286 (1974), edited by Stephen Gillers and myself, with a foreword by Anthony Lewis, a link to the Center on Law and Security’s conference on secrecy and government.

of wholly secret trials (McCarthy also held secret hearings, but they were not criminal cases); the sequestration of prisoners in Guantanamo, an enclave claimed to be wholly beyond the reach of courts; and torture and its handmaiden, rendition, which need no comment.

A third new element, related to the first two, is the apparently permanent nature of today's crisis. We have had long wars, both declared and undeclared, but there was little doubt about when the fighting ended, either by surrender, a treaty, or a withdrawal from the fray. Many have observed that these benchmarks very likely will not exist in the "war against terrorism." If this is true, what will be the consequences for American society, including the relationship between secrecy and openness?

A fourth new element, and an encouraging one, is the greater willingness of American lawyers to represent those accused of terrorism or related crimes. We have had pariah groups in the past – the Bolshevik sympathizers during and after World War I, the Japanese-Americans transported from the West Coast to interior camps, and the accused Communists during the McCarthy period. There were always a few lawyers who, at risk to their livelihoods and reputations, were prepared to defend these unpopular clients.

But today the number of such lawyers is much larger. It includes lawyers in more established firms who are committed to advancing constitutional interests, including fair process and transparency when government acts. It also includes many lawyers in what we call public interest legal organizations. The ACLU, for example, had about 10,000 members and one staff lawyer on its national staff in the 1950s, while today there are approximately a half million members and about 200 lawyers (which does not include the many lawyers in its state affiliates). Thus, the organization recently has

been far better prepared to defend civil liberties, including the public's right to know, than in prior crises.

To the extent that we succeed in gaining access to government "secrets," the new knowledge will, as Karen Greenberg aptly said in closing the conference, bring "certain responsibilities. Knowing is scary and sometimes we just do not want to know." But we must persevere nonetheless because the democracy of our country is at stake.

Prof. Norman Dorsen is Stokes Professor of Law and Counselor to the President, New York University. General Counsel (1969-1976) and President (1976-1991), American Civil Liberties Union.

A grayscale, blurred image of a person's face, blindfolded with a cloth. The person has a beard and is looking slightly upwards. The image is centered and serves as the background for the text.

**PRIVACY IN THE AGE OF
NATIONAL SECURITY**

NOVEMBER 14, 2007

Privacy in the Age of National Security: Participant Biographies; November 14, 2007

Valerie E. Caproni has been the general counsel of the FBI's Office of the General Counsel since 2003. She was previously regional director of the SEC's Pacific Regional Office, where she oversaw enforcement and regulatory programs in the nine far western states, managing a staff of approximately 250 lawyers, accountants, and examiners in Los Angeles and San Francisco. While at the SEC, Ms. Caproni dramatically increased the cooperation between the commission and federal prosecutors in order to maximize the impact of enforcement actions. Previously, she was counsel at the law firm of Simpson Thacher & Bartlett, specializing in white collar criminal defense and SEC enforcement actions; chief of the Criminal Division of the U.S. Attorney's Office, Eastern District of New York; and clerk for the Hon. Phyllis Kravitch, United States Court of Appeals, Eleventh Circuit.

Bryan Cunningham has extensive experience as a cybersecurity and intelligence expert, both in senior U.S. government posts and the private sector. Cunningham, now a corporate information and homeland security consultant and principal at the Denver law firm of Morgan & Cunningham LLC, most recently served as deputy legal advisor to National Security Advisor Condoleezza Rice. At the White House, Cunningham drafted key portions of the Homeland Security Act. He was deeply involved in the formation of the National Strategy to Secure Cyberspace as well as numerous presidential directives and regulations relating to cybersecurity. He is a former senior CIA officer and federal prosecutor, founding co-chair of the ABA CyberSecurity Privacy Task Force, and a recipient of the National Intelligence Medal of Achievement for his work on information issues. Cunningham holds a top secret security clear-

ance and counsels corporations on information security programs. He also counsels information security consultants on how to structure and conduct their assessments and remediation to mitigate potential liability.

Barton Gellman is a fellow at the Center on Law and Security and the special projects reporter on the national staff of *The Washington Post*. Previously, he completed tours as diplomatic correspondent, Jerusalem bureau chief, Pentagon correspondent, and D.C. Superior Court reporter. He shared the Pulitzer Prize for national reporting in 2002 and has been a jury-nominated finalist (for individual and team entries) three times. His work has also been honored by the Overseas Press Club, the Society of Professional Journalists (Sigma Delta Chi), and the American Society of Newspaper Editors. He is author of *Contending with Kennan: Toward a Philosophy of American Power*, a study of the post-World War II "containment" doctrine and its architect, George F. Kennan.

Todd Gitlin is professor of journalism and sociology and chair of the Ph.D. program in communications at Columbia University. He is the author of twelve books, including, most recently, *The Bulldozer and the Big Tent: Blind Republicans, Lame Democrats, and the Recovery of American Ideals*. He has contributed to many books and published widely in periodicals, online magazines, and scholarly journals. He is an editorial board member of *Dissent*, a contributing writer to *Mother Jones*, a member of the board of trustees of openDemocracy.net, and a regular contributor to TPMCafe.com. He was the third president of Students for a Democratic Society, in 1963-64, and coordinator of the SDS Peace Research and Education Project in 1964-65, during which time he helped

organize the first national demonstration against the Vietnam War. During 1968-69, he was an editor and writer for the *San Francisco Express Times*, and through 1970 wrote widely for the underground press. He is presently a member of the board of directors of Greenpeace USA.

Karen J. Greenberg is the executive director of the Center on Law and Security. She is the editor of the *NYU Review of Law and Security*, co-editor of *The Torture Papers: The Road to Abu Ghraib*, and editor of the books *Al Qaeda Now* and *The Torture Debate in America* (Cambridge University Press). She is a frequent writer and commentator on issues related to national security, terrorism, and torture and has authored numerous articles on the United States and Europe during World War II. She is a former vice president of the Soros Foundation/Open Society Institute and the founding director of the Program in International Education. She is an editor of the Archives of the Holocaust, Columbia University Series, and has served as a consultant to the National Endowment for the Humanities, the NY Council for the Humanities, the NYC Board of Education, and USAID.

Stephen Holmes is a faculty co-director at the Center on Law and Security and the Walter E. Meyer Professor of Law at the NYU School of Law. His fields of specialization include the history of liberalism, the disappointments of democratization after communism, and the difficulty of combating terrorism within the limits of liberal constitutionalism. In 2003, he was selected as a Carnegie Scholar. He was a professor of politics at Princeton from 1997 to 2000, professor of politics and law at the University of Chicago's law school and political science department from 1985 to 1997, and taught at Harvard University's department of government from 1979 to 1985. He was the editor in chief of the *East European Constitutional Review* from 1993-2003. He is the author of *Benjamin Constant and the Making of Modern Liberalism* (Yale University Press, 1984), *The Anatomy of*

Antiliberalism (Harvard University Press, 1993), *Passions and Constraint: On the Theory of Liberal Democracy* (University of Chicago Press, 1995), and co-author (with Cass Sunstein) of *The Cost of Rights: Why Liberty Depends on Taxes* (Norton, 1999). His most recent book, *The Matador's Cape: America's Reckless Response to the War on Terror* (Cambridge University Press) was published in spring 2007.

Jeff Jonas is chief scientist of the IBM Entity Analytic Solutions group and an IBM distinguished engineer. He is responsible for shaping the overall technical strategy of next generation identity analytics and the use of this new capability in IBM products. His innovations have received coverage in such publications as *The Wall Street Journal*, *The Washington Post*, *Fortune*, and *Computerworld*, and have been featured on ABC's *Primetime*, The Discovery Channel, The Learning Channel, and MSNBC. Mr. Jonas is a member of the Markle Foundation Task Force on National Security in the Information Age and actively contributes his insights on privacy, technology, and homeland security to leading national think tanks, privacy advocacy groups, and policy research organizations, including the Center for Democracy and Technology, the Heritage Foundation, and the Office of the Secretary of Defense Highlands Forum. Most recently, he has been named a senior associate to the Center for Strategic and International Studies.

Vivian Maese is a senior vice president and associate general counsel at NYSE Euronext, where she manages a team of lawyers and professionals in the Office of the General Counsel. Her responsibilities include the U.S. trading businesses, securities market structure, technology, intellectual property, and market data. She began her career on Wall Street working for Norman Schvey, a pioneer in the development of unit investment trust products at Merrill Lynch. From Merrill Lynch, Maese joined Salomon Brothers Inc., which became Citigroup. She

worked there for over 20 years providing industry-leading expertise in intellectual property, technology, and patent law. She served the securities industry as a member of the Securities Industry and Financial Markets Association's Technology and Regulatory Committee and was founding chair of the Intellectual Property Committee. Maese has been a member of the New York Bar Association's Computer Law Committee, Women in Law Committee, and Executive Committee. In addition, she founded the Wall Street Computer Law and Intellectual Property Roundtable. She is a frequent panelist at industry meetings and has published on legal issues related to technology and intellectual property.

Declan McCullagh is the chief political correspondent and senior writer for CNET's News.com. An award-winning journalist, McCullagh writes and speaks frequently about technology, law, and politics. He was the Washington bureau chief for Wired News from 1998 to 2002. Previously he was a reporter for *Time*, *Time Digital Daily*, and *The Netly News*, as well as a correspondent for *HotWired*. His articles have appeared in scores of publications including *The Wall Street Journal*, *The New York Times Magazine*, *Playboy*, *George*, *The New Republic*, and the *Harvard Journal of Law and Public Policy*. He has appeared on NPR's *All Things Considered*, ABC News's *Good Morning America*, NBC News, Court TV, and CNN. Since 2002, he has been an adjunct professor of law at Case Western Reserve University. He is an adjunct professor at American University in Washington, DC, where he has taught a graduate journalism class. McCullagh moderates Politech, a mailing list he founded in 1994 that looks broadly at politics and technology. He was the first online reporter to join the National Press Club, he participated in the first White House dot com press pool, and was one of the first online journalists to receive credentials from the press gallery of the U.S. Congress.

Burt Neuborne is the legal director of the Brennan Center for Justice at the NYU School of Law. The Brennan Center, established in 1994 by the law clerks to Justice William Brennan, Jr. to honor his monumental contribution to American law, seeks to link the academic resources of a great law school and the practical skills of the bar in an effort to develop pragmatic approaches to problems that have resisted conventional solutions. Neuborne was appointed NYU law school's first John Norton Pomeroy Professor of Law in 1991 and received the university-wide Distinguished Teacher Award in 1990. He has been one of the nation's foremost civil liberties lawyers for 30 years, serving as national legal director of the ACLU, special counsel to the NOW Legal Defense and Education Fund, and as a member of the New York City Human Rights Commission. He challenged the constitutionality of the Vietnam War, pioneered the flag burning cases, worked on the *Pentagon Papers* case, worked with Justice Ruth Bader Ginsburg when she headed the ACLU Women's Rights Project, and anchored the ACLU's legal program during the Reagan years. Among Neuborne's best-known scholarly works is the two-volume *Political and Civil Rights in the United States* (with Norman Dorsen, Sylvia Law, and Paul Bender).

Robert O'Harrow, Jr., is the author of *No Place to Hide* and a reporter for the financial and investigative staffs of *The Washington Post*. He has carved out a data-privacy beat and uncovered stories about the use of information that has led to changes in state and federal law. In 2000, O'Harrow was a finalist for a Pulitzer Prize. He was a recipient of the 2003 Carnegie Mellon Cybersecurity Reporting Award.

Stephen Schulhofer is the Robert B. McKay Professor of Law at the NYU School of Law and one of the nation's most distinguished scholars of criminal justice. He has written more than 50 scholarly articles and six books. His most recent book, *The Enemy Within: Intelligence*

Gathering, Law Enforcement and Civil Liberties in the Wake of September 11, written for The Century Foundation's Project on Homeland Security, has attracted wise attention as a careful and balanced critique of domestic measures being implemented as part of the "war on terrorism." He has written on police interrogation, the self-incrimination clause, administrative searches, drug enforcement, indigent defense, sentencing reform, plea bargaining, capital punishment, battered spouse syndrome, and other criminal justice matters. His current projects include an investigation of the growing practice of trying juveniles in adult court and an analysis of recent developments in the Supreme Court's interpretation of core Fifth Amendment principles. Previously the Julius Kreeger Professor of Law and director of studies in criminal justice at the University of Chicago Law School, Schulhofer was also the Ferdinand Wakefield Hubbell Professor of Law at the University of Pennsylvania. He clerked for two years for U.S. Supreme Court Justice Hugo Black. Before teaching, he also practiced law for three years with the firm Coudert Freres, in France.

Geoffrey Stone has been a member of the law faculty of the University of Chicago Law School since 1973. He served as dean of the law school from 1987-1993 and as provost of the university from 1993-2002. He served as a law clerk to Judge J. Skelly Wright of the U.S. Court of Appeals for the District of Columbia Circuit and to Justice William J. Brennan, Jr., of the U.S. Supreme Court. Stone teaches primarily in the areas of constitutional law and evidence and writes principally in the field of constitutional law. His most recent books are *Top Secret: When Our Government Keeps Us in the Dark* (Rowman & Littlefield, 2007) and *War and Liberty: An American Dilemma* (W.W. Norton, 2007). His book *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism* (2004) received the Robert F. Kennedy Book Award for 2005, the Los Angeles Times Book Prize for 2004 for the best book on

history, the American Political Science Association's Kammerer Award for 2005 for the best book on political science, the Hefner Award for the best book on the First Amendment, and Harvard University's 2005 Goldsmith Award for the best book on public affairs. Stone is working on a new book, *Sexing the Constitution*, which will explore the historical evolution in western culture of the intersection of sex, religion, and law.

Matthew Waxman, an expert in the domestic and international legal aspects of fighting terrorism, is an associate professor of law at Columbia Law School. He clerked for Associate Supreme Court Justice David H. Souter and Judge Joel M. Flaum of the U.S. Court of Appeals for the Seventh Circuit, and served in senior positions at the U.S. State Department, Department of Defense, and National Security Council. Professor Waxman was a Fulbright Scholar to the United Kingdom, where he studied international relations. He has authored several books on the use of military force as an instrument of American foreign policy.

Lawrence Wright is an author and screenwriter, staff writer for *The New Yorker* magazine, a fellow at the Center on Law and Security, and a Pulitzer Prize winner for his book on al Qaeda, *The Looming Tower: al-Qaeda and the Road to 9/11* (Knopf, 2006). *The Looming Tower* was named one of the top ten books of 2006 by both *The New York Times* and *The Washington Post*, and was nominated for the 2006 National Book Award. A portion of that book, "The Man Behind Bin Laden," was published in *The New Yorker* and won the 2002 Overseas Press Club's Ed Cunningham Award for best magazine reporting. Wright has won the National Magazine Award for Reporting as well as the John Bartlow Martin Award for Public Interest Magazine Journalism.

Privacy: Then and Now

Panelists:

Valerie Caproni, Robert O’Harrow, Jr.,
Prof. Geoffrey Stone

Moderator:

Prof. Burt Neuborne



Prof. Geoffrey Stone. *Photo by Dan Creighton.*

Karen J. Greenberg:

People often talk about the threats to our privacy under the Patriot Act and other Bush administration programs, but the actual notion of what privacy is – whether we have a right to it, why we think we have a right to it, and whether we even want it – seems to be somewhat up for grabs. The issue brings together the government, the corporate sector, the medical sector, and many diverse specialties that we do not usually combine in the same conversation. I see today’s discussion as the beginning of a long-term dialogue about these ideas, which hopefully will come into focus as we talk about them.

Privacy is a generational issue, and the way in which policymakers and commentators address it today may be irrelevant sooner than we think. My mother will not use her credit

card at the supermarket because she does not want people to know what groceries she buys. That is her notion of privacy. One of my brothers will not go through the E-ZPass lane at the tollbooth because he does not like the idea of anybody knowing where he has been or where he is going. My daughter and her friends, however, post photos and trade notes on Facebook. They are an open book to one another and they do not care. They have a very different conception of what privacy should be.

I think that the idea of protecting privacy, as we understand it, is already outdated. Over time, we should begin to understand a new concept of privacy that is very much within us.

Prof. Burt Neuborne:

We are going to ask difficult and theoretical questions about the nature of privacy and how it

evolved as an idea. In thinking about the future, this panel will also discuss the notion of what privacy will look like in the technologically explosive world of the 21st century, why we should care, and what parameters should be imposed upon it.

Valerie Caproni:

Given my position as general counsel for the FBI, I suspect that few people will be surprised when I say that the primacy of privacy has not been sacrificed to the demands of national security or law enforcement. I do think that the topic needs to be discussed and that there must be public debate about it.

I recognize that many of the panelists today feel that the accretion of power in the executive branch has endangered privacy and that we

seem to have an endless desire to collect information on citizens.

Nevertheless, it is my strong belief that the FBI is striking the correct balance between privacy and security (I do not have sufficiently in-depth knowledge to talk about other federal agencies). Too often, the debate is phrased in terms of an either/or proposition: you can either respect privacy or have national security, but not both. I reject that notion. The question is one of balance.

From the Bureau's perspective, the notion of balancing security and privacy is nothing new. Benjamin Franklin said, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." I think we respect the notion of a middle ground.

For all of our almost 100 years of existence, the FBI has been in the business of balancing national security and civil liberties. We view privacy as one element of civil liberties.

There have admittedly been times in our history when we did not do a good job of balancing those equities. The abuses of the 1960s and '70s that led to the Church Committee in the Senate and the Pike Committee in the House are prime examples of the balance being askew, but things have changed since those days. The agents now working at the Bureau were children in the days of the counterintelligence programs known as "COINTELPRO." Those programs are not a part of any current agent's history.

Four significant developments came out of those errors and have radically changed how the Bureau does business. They continue to establish an environment that makes sure the Bureau stays in the middle ground between privacy and security, notwithstanding how many view the



“Too often, the debate is phrased in terms of an either/or proposition: you can either respect privacy or have national security, but not both. I reject that notion.”

Valerie Caproni

effects of the Patriot Act and other post-9/11 legislative changes.

First, Congress passed the Privacy Act and various other statutory schemes that protect private information held by third parties. The Privacy Act provides a broad statutory framework for government collection of personally identifiable information. While the Bureau is exempt from certain portions of the Act, its existence broadly affects

how we look at the collection of such information. We have been doing privacy impact analysis on every new major recordkeeping system that we have created since the year 2000 – before it was statutorily required – because we understand the concerns about collecting personally identifiable information. We continue to do such analysis even on our national security systems, which is not statutorily required. It is important to us to look at these systems as they are put into place to ensure that we have appropriate controls and protections built into them. In mid-2006, we created within the Office of General Counsel a unit of lawyers that does nothing but privacy and civil liberties work.

In addition to the Privacy Act, Congress has passed a number of laws that protect various types of information, from telephone records – which have been expanded to include electronic communication and Internet records – to educational and financial records. These laws do not prevent us from getting access to the information, which we need in order to do our jobs, but they generally impose a level of process into our obtaining that access. The process and the controls built into it vary depending on how private the information is.

The second major change since the Church-Pike Committees is the attorney general guide-

lines that govern how the FBI does its work. Before then, back in the '60s, there really were no guidelines. The Bureau could do what it wanted to do. There are now guidelines that are internal to the Justice Department but affect how we do business in a very real way. They change from attorney general to attorney general. Some changes that John Ashcroft made after 9/11 received a fair amount of press attention. But at their core, they haven't changed significantly since they were first promulgated in the late 1970s.

The guidelines require intrusive investigative activity by the FBI to be based on some factual predicate. The subject of the investigation must be someone we have an interest in investigating – a criminal, a terrorist, or a spy. Broadly, the guidelines also require a graduated approach, so that more intrusive techniques can only be used if there is a more substantial predicate. If we know very little, we can use open-source reporting to gather information to figure out if we should look more closely at someone. On the other hand, if we have fairly substantial information that the person is a criminal, terrorist, or spy, then we can use very intrusive techniques, up to and including electronic eavesdropping.

The agency guidelines also mandate that the exercise of First Amendment rights cannot be the sole basis for an investigation. Somebody can protest the Iraq War all they'd like, but that cannot form the basis of an FBI investigation if it is all we know about the person. These limitations collectively require the FBI to take a graduated and intelligent approach to who we are investigating and, therefore, who we are collecting personal information about.

The third development that followed the Church-Pike hearings was the enactment of the Foreign Intelligence Surveillance Act, or "FISA." There are a substantial number of people who think that FISA was trampled by the National Security Agency's Terrorist Surveillance Program. There are also a number of people who believe the amendments to FISA that were passed in August 2007 did grave harm to its statutory structure. But from the FBI's perspective, FISA did one important thing. It gave us a legal structure with court oversight to get orders to authorize electronic surveillance within the United States for national security purposes. The authority provided in FISA largely paralleled the authority that had been previously provided by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to electronically eavesdrop during criminal investigations.

This change of law was incredibly important, because the existence of judicial oversight over our most intrusive activities seems to generate trust by the American people. FISA provided that. It gave us a court to go to for our national security surveillance. Since the law's enactment, the FBI has

used its framework exclusively to accomplish national security eavesdropping on people inside the United States. Nothing in the new amendments changes that. It is still the basic Bureau structure. If we are eavesdropping in the United States, on someone who is in the United States, we get a court order.

The fourth change since Church-Pike is that there is now substantially enhanced oversight of the activities of the FBI and the balance of the intelligence community. The Senate and the



“We have to realize that data flows together and that billions of records are being collected The corporations and governments that have access to it are able to look at us in a way that few understand.”

Robert O'Harrow

House now both have intelligence committees that are regularly briefed on the activities of the intelligence community, including some of the Bureau's most sensitive investigations. We also have a vigorous inspector general system. The inspector general provides needed (if, from my position as general counsel, sometimes painful) oversight of our activities.

These changes have collectively served the United States well in ensuring that the government limits its intrusion into individual rights. I think the balance right now is a good one, although the pendulum seems to be swinging slightly back and forth. Given the massive increase in the amount of information that we can collect quickly and easily, this is a necessary debate.

Prof. Burt Neuborne:

Mr. O'Harrow, what is your sense of the existing state of privacy in the United States, how we got here, and where we are going?

Robert O'Harrow:

I want to challenge all of us to think about the issue we're discussing in a different way, because we are not actually talking about privacy. The word "privacy" is like tofu. All of us are applying different flavors to it based upon preconceptions and things we have read. What we are really talking about are some very old, traditional American values. The key is autonomy. What is the state of autonomy for the individual in America, relative to corporations and relative to the government?

Some of this will sound redundant, but my argument, based on research and speaking with many people in the government and the private sector, is that it is important to take a broader perspective. We are in the midst of a data revolution that has been occurring for three decades. We will look back on this era as one of the great technological revolutions in American and world history. It poses core challenges that go far beyond the issues we look at in a microscop-

ic way: how FISA is working, how our social security number is being used, whether or not we should have a camera watching us, and whether the government can eavesdrop. We think about what our banks are doing with our information and what the grocery stores are doing.

What we have to try to do, and what hopefully society will eventually come to, is realize that we cannot look at these individual things. We have to realize that data flows together and that billions of records are being collected about every American. That information flow is creating a composite portrait of us that is getting a higher and higher resolution so that the corporations and governments that have access to it are able to look at us in a way that few of us understand. That is the power I'm talking about, and that is the question of autonomy.

When the corporations who have this information can use insights about us to make decisions, and when they work with the government to protect us or to root out terrorists or prevent crime, how do we feel about that? There are benefits and a clear utility. I have not yet come across a technology in a data-collection system without a clear service, convenience, or new level of security being offered. That is something we need to accept. It would be foolish to turn our backs on these benefits. We are not Luddites.

But what we are not being told, either by the data collectors or the government clients, is the power that it is giving them to look into our behavior, connections, friends, habits, and inclinations, and to use that information to make decisions about us without our knowledge. To me, that is the fundamentally offensive thing. We are not full participants in the outcome of this revolution, so it is not about privacy but rather about autonomy. It is about a shift of power.

Much of the current debate about national security is focused on the minutiae. For example, we heard about the NSA eavesdropping

from a good and important story in *The New York Times*. I would bet that 90 percent of us, when we hear the word “eavesdropping,” think of somebody with headphones on. We think they’re listening, right? But that is not what is happening and it is not the point. It is completely beside the point. Yet that idea is defining the terms of the debate and the coverage in the media.

I think we are going to find in a few years hence, when the full story about what the NSA is doing comes out, that it is not eavesdropping on a few thousand people in the way we think of it. It is actually collecting data about the phone calls of millions of Americans, about millions of credit reports, about buying habits, and conducting link analysis of tens of millions of people. In other words, the NSA program is not about phone calls. It is about the data on all of us. That is probably only a tiny slice of the data collection and analysis that is going on.

I think we are going to find that what the NSA is doing is perfectly legal because FISA did not contemplate the data revolution when it was written. It contemplated headphones. The present reality is that the government has easy and instant access to records that are astonishingly detailed: the people we are associated with, everywhere we have lived, the things we buy, and our credit reports. There is a great utility there but it is a source of power that is largely unchecked because we have not gotten our minds around what it means.

There is oversight. There are oversight mechanisms that were established after the abuses of the ’60s and ’70s. But I am doing a rolling investigation of fraud, waste, and abuse in government contracting, and I will tell you that execution of the oversight is incredibly thin. The ability of any oversight committee to understand, let alone follow through on, the use of billions of records is absolutely minimal. It does not mean that use of those records shouldn’t occur – there is a utility and it is a debate that we need to have – but the idea that there is

sufficient oversight is not true. The people on Capitol Hill are as flummoxed by the data revolution as the rest of us are.

That is not to say that the FBI is misusing this in a systematic way, but it is to say that they, like major corporations and other government agencies, are tapping into the data revolution in a way that the rest of us do not fully understand.

We need to see what the government is doing and have a check on that power to ensure that we look out for the individual as we strive to improve security, because that’s what this country is about.

Prof. Burt Neuborne:

Prof. Stone, we have heard two perceptions of the same truth. What is your sense of how we as a country got here and where we are likely to be going?

Prof. Geoffrey Stone:

I would like to make three points. First, we are living in a situation that is completely unprecedented and previously unimaginable in terms of the challenge of reconciling privacy with national security. Part of that is because the legitimacy of the government’s interest in intruding on privacy is greater by a quantum difference than it has ever been before. Second, the government’s capacity to invade privacy is similarly greater than it has ever previously been. Third, those of us who worry about privacy need to think hard and quickly about why we care about it, and figure out whether there is any way to restrain the tsunami that is already upon us.

The conflict between safety and privacy goes back to the beginning of the nation. The Fourth Amendment was enacted precisely to try to deal with the concern that government officers would engage in unreasonable searches and seizures. That was well understood by the Constitution’s framers. Government has always had a desire to know more about what its citi-



Valerie Caproni. *Photo by Dan Creighton.*

zens and others are doing so it can protect the nation. But the situation we face today is unprecedented in terms of the legitimacy of that need because, essentially, we face a completely unique threat.

For the first time in our history, we face the threat that a small number of rogue individuals have the capacity to inflict enormous damage through conventional chemical, biological, or nuclear weapons. There is also no practical way to deter them. Unlike the Soviet Union, which could be deterred by the threat of retaliation, there is no realistic deterrence possible when dealing with committed terrorists, particularly suicide bombers.

The need to prevent therefore becomes critical. The only practical way to protect ourselves is to stop these events before they occur, and the only way to do that is to know who is doing what, when, where, and why. The legitimate interest in knowing what everyone is saying and doing all of the time in order to find the needle in the haystack – to find those who may have access to a nuclear, biological, or chemical weapon – becomes the only effective defense against the possible death of tens or hundreds of thousands of Americans. So the incentive for the government to expand its capacity to gather

and collect information as aggressively as possible is completely understandable.

The second point is that the government's ability to gather information is entirely unprecedented. Because of the computer and data revolutions, the government's ability to gather and collate information is different than it has ever been before. We are no longer talking about a world in which you need a three-dimensional person to search a home or even to listen, as Mr. O'Harrow said, in a pair of headphones. We are now talking about a situation

in which the government can gain access to everything we do electronically – every phone call, e-mail, purchase, every time we go through an EZPass lane, essentially everything we do. There are cameras on street corners. Bank transactions can be gathered, collated, and identified with each and every one of us. None of this was possible even a few years ago.

The government's capacity to gather information now matches what it perceives to be its need. Faced with these two realities, those of us who believe that privacy is important need to articulate, explain, and justify why the government should be restricted in its legitimate efforts to us safe. This is a challenging question.

If we think about why the framers were worried about searches and seizures, they had in mind a group of government officials coming into your home and rummaging around in your desk. They were concerned about disruption, humiliation from having to stand there while public officials make a mess of your home and embarrass you, and invasion of property rights. The kind of surveillance we are talking about now involves none of these issues. It is invisible. There is no actual disruption of our lives by the fact that the government is gathering this information. There is no humiliation because we

do not know that it is occurring. There is no invasion of our property rights because the government is not physically coming into our homes and interfering with anything we think of ourselves as “owning” in a conventional sense.

That is why courts, including the Supreme Court, for the first 40 years of electronic surveillance essentially said that such surveillance does not constitute a search within the meaning of the Fourth Amendment. It was not until 1967 that the Supreme Court had the idea that we should think about privacy as an independent value protected by the Fourth Amendment. But it is important for us to remember how recent a phenomenon this is.

The difficulty is that although many people say they care about privacy and autonomy they cannot explain why those values are worth protecting relative to national security threats. Why should we endanger ourselves to protect this thing called “privacy”? Some people would say, “What I do is none of the government’s or anyone else’s business. I should be able to do whatever I want. Unless I’ve done something wrong, I should be free to not be under surveillance.” Others would answer, “I don’t care if the government taps my phone calls or knows my bank records. I am not doing anything wrong. Let them go look for the needle – I’m the haystack.” The only people who have anything to fear, they think, are those who are doing something wrong and who should not have any right to hide it. That is not a crazy response and it is probably the most common. There needs to be some explanation, then, as to why it is not an adequate response to the problem.

One response is that the government gathers enormous amounts of information, and not only about the bad guys. What does the government do with that information? Does it simply disregard it? Are we not at all prejudiced by the fact that the government gathers huge amounts of unnecessary information? Or is the information accessible and being retained and used for all sorts of other reasons that might be problematic to us? Those are questions that we need to talk about, and we need to ask whether safeguards could be devised.

The final aspect, and I think the most important one, has to do with the definition of a self-governing society. In such a system, the citizen has to understand that he or she is the ruler, the governor, and not subject to the constant oversight and surveillance of the government,

which is essentially the servant. To the extent that we get used to the idea that everything we do, everything we say, and every transaction we enter into is the government’s business, we run the risk of seriously undermining, in the long run, the relationship between the individual and the state that is essential to an effective self-governing society. But that, too, is an argument that needs to be developed, fleshed out, and ultimately debated to see

whether we are prepared to make ourselves less safe in order to preserve those values.

Prof. Burt Neuborne:

My skepticism about the way private corporations use the idea of privacy is fueled by 11 years of experience litigating Holocaust cases. The Swiss banks deployed a highly intellectualized vision of privacy to justify their refusal to



“To the extent that we get used to the idea that everything we do, everything we say, and every transaction we enter into is the government’s business, we run the risk of seriously undermining the relationship between the individual and the state.”

Prof. Geoffrey Stone

provide information necessary for a decent remedial system there. Switzerland essentially served as a haven where drug dealers and dictators put their money in ways that made it impossible for the world to police. If you have a place where you can stick your money and then wave the flag of privacy, you can eviscerate enforcement mechanisms. We now have treaties with Switzerland and all sorts of efforts to gain information, but I am skeptical about how well they work.

German insurance companies used privacy as a justification for not telling people about the number of Holocaust-era policies that remain unpaid. After the state of California passed a statute requiring them to make the information publicly available in order to do business there, the Supreme Court struck it down in 2003 on the grounds that it interfered with European conceptions of privacy bound up in their data collection mechanisms.

So I have a tremendous ambivalence. I am sure that companies will abuse the data if they get it. On the other hand, if we allow this major deployment of a privacy notion, I am convinced that they will abuse that, too.

So the question is, how do we talk about information flow, with information constituting power in the 21st century? Mr. O'Harrow, do you want to answer the question that Prof. Stone posed? Why should we care about privacy in a world where everybody knows everything about everyone else anyway?

Robert O'Harrow:

Forget everything you have heard about privacy being over. The reality is we are at the very beginning of the data revolution. The issue is not about stopping data flows and the utilities that bring us so many conveniences, services, and increased security. It is about understanding that revolution, first and foremost, and then coming up with some sort of framework to decide how we want this information applied, how we want these insights to be used, and how

we punish people who misuse them.

To answer Prof. Stone's broad question, think about the 1940s and '50s. Try to imagine how it was when people took for granted that shiny new cars, increases in steel production, and the chemicals produced in factories across the country were inherently good things. Regular people did not think seriously about the impact of all that production. It took a generation, but it has become mainstream to think about recycling and air quality.

This kind of thinking can be applied to the data revolution, so here is my answer: I think that privacy matters because we have to create structural incentives over the long run for the government to behave in a way that fulfills our expectations for independence and autonomy.

We have to demand accountability now and every step of the way so that the government is forced to think about these things in ways that it otherwise would not. Why would the FBI police itself, limit itself, make life harder for itself, and come up with an analysis of how it is using information unless "we the people" expect and demand it? We as a society are going to have to demand it so the government doesn't go astray. That is not against the government but rather for it. It will make society operate more efficiently in protecting ourselves and improving security.

When we talk about national security, it is amazing how often the government with the new tools that it has access to and the corporations who provide these services are posed as inherently good – that they are going to self-police and act in benign ways. That is a canard. It is not going to happen. Individuals, corporations, and governments will often go astray, not because they are bad but because they are often not thinking clearly about the issues at stake.

The government ought to show why they need more information and why they need to get into our heads, our backgrounds, and our histories. We should demand that without

getting in the way of their using it in real ways to protect us.

Prof. Burt Neuborne:

Ms. Caproni, what two things would you do to improve the balance between privacy and security without losing the value of privacy?

Valerie Caproni:

Let me try a concept, which this conversation has helped crystallize. From the discussion this morning, you would think that we within the FBI or the government writ large are taking in massive amounts of personal information about everyone here today – that I could go back to my computer, run your names, and know that you bought oatmeal yesterday or that you went over the Triborough Bridge two days ago.

That is not accurate. There may be one person here whose oatmeal we know about, but probably not. We probably have not collected any record on anyone in this room, through a national security letter or otherwise. I am willing to bet that there is no one here about whom I have an iota of information. Yet listening to this discussion, you would think that we know everything about all of you.

I think the reason for the disconnect is partly because of the unfortunate reality that we are not willing to go entirely public about exactly what we do, what we collect, and how we collect it. There are people, who, if they had that information, would alter their behavior to stay off our radar so that they could continue to do bad things.

I have struggled with how we could make more information available to counteract some of the fears that the government is sucking up information on many people for improper purposes – purposes that would recall the era when we were going after people for political reasons, or for what they said rather than what they were planning to do. I do not have a cure for that.

We have made some changes as part of the reauthorization of the Patriot Act. We now pro-

vide numbers regarding how many people we have collected information on through national security letters (or “NSLs”). It is a bit of a blunt statistic but it is one. To some extent, the change was written into the reauthorization in response to one of Mr. O’Harrow’s articles in *The Washington Post* about an upsurge in the use of NSLs. National security letters allow us to secretly collect telephone and financial records relevant to an investigation. There was some suggestion that we were using them in a very broad way to collect massive amounts of data. The solution was to declassify the number of people on whom we collect data each year. It is not a perfect solution but it is not bad. The number, published yearly, is not substantial. That is why I can say with a great deal of confidence that the likelihood of anybody in this room having been the subject of a national security letter is practically zero.

Robert O’Harrow:

One of the problems with the debate we have been having for a couple of years is that it is suffused with hyperbole. The government is inappropriately accused of being Big Brother. Critics sometimes debate the issue as though there are no checks, and that is incorrect.

Ms. Caproni’s response strikes me as overly narrow and, as a result, problematic. How does the government address the fact that the CIA, for example, has a contract with ChoicePoint, a data broker that maintains about 20 billion records, about virtually every American adult? The records are becoming more of a commodity than they are anything else, so ChoicePoint provides analytics as a value-added service, and even those are in an early stage. The CIA, the FBI, every other law enforcement agency in the government, and probably every intelligence agency, have access to records that would have been impossible to get 20 years ago on a regular basis.

This means that searches on every one of us here can be conducted legally because it is a

round-the-clock, fee-based service. That kind of power is the tip of the iceberg of information that is available publicly, legally, and, in many cases, ethically and legitimately. But it is a shift. A dramatic revolution is occurring.

Valerie Caproni:

That is true, I don't disagree. ChoicePoint is a huge data aggregator. They have, I suspect, information on everyone here. We have access, as do the CIA, *The Washington Post*, and employers generally. ChoicePoint searches are done all the time. There is a business model and an insatiable desire for that kind of information.

The distinction I draw, and maybe it is too cute by half, is the difference between us at the FBI having access to information via ChoicePoint, LexisNexis, Westlaw, or other services and our collecting the information and bringing it into our databases so that we can slice it and dice it as we see fit. The latter is governed by the laws that control the government's collection of information. If we are simply asking ChoicePoint to run someone through their system to tell us what they know about them, we are accessing information in the same way that everyone else within the United States can. Whether ChoicePoint should be able to aggregate all that information is absolutely subject to public debate, but it is not unique to the government. What we are doing is accessing collected information that is available to everyone else, and on the same terms.

Robert O'Harrow:

I do not mean to raise this issue, even in the slightest, as an attack on the government or its use of information. As you say, I have access to

it. In fact, part of the reason I began writing about data was because I got very good at accessing it and I felt like the public ought to know what was happening. I am just trying to point out that we need to do some values testing and weigh what this means, not only for the present but for 10 or 20 years from now when the richness of the data has become staggeringly more dense.

Prof. Geoffrey Stone:

It is our responsibility to distrust the FBI, because they work for us. We know, from the experience of over 200 years, that individuals with the levers of government authority will abuse that authority if given the opportunity. Often they mean well, often they don't, but they will abuse it. Therefore, the trust is not a two-way street, nor should it be.

Part of the difficulty at the moment is that we do not have rules, regulations, laws, or oversight that even touch the surface of the government's ability to utilize this information, whether they get it by their own

investigation or pick it up from ChoicePoint. In my view, it makes absolutely no difference.

To equate the government's use of this information with the private sector's ignores the fact that we have a Constitution. The Constitution regulates the government, not the private sector. There are good reasons for that. The government has certain capacities to abuse power that the private sector does not. We can deal with the private sector through legislation, and we should, but it is no answer to concerns about the government's access to information to say that other people have access to it too. They are two completely different issues from the standpoint of our legal system.



“The feeling that we are being watched, whether or not we actually are, creates a deterrence on non-conventional behavior for which our culture will eventually pay a price.”

Prof. Burt Neuborne

It seems to me there was a moment in history when we went wrong in a constitutional sense. It was profoundly wrong for the Supreme Court to adopt the notion that there is no constitutional invasion of privacy when the government gathers information about someone without intruding upon his property and can say that he has indicated an indifference to the privacy of the information.

The typical analogy would be someone walking down street wearing all black. He has exposed the fact he is wearing all black to the public. If a police officer wants to write that down because it is relevant to some investigation, there is no Fourth Amendment issue. The Court took that to say that if you have exposed your financial transactions to employees at a bank who are strangers to you, or your reading purchases to the employees of a book store, library, or Web site, all of whom are strangers to you, then you are indifferent to the privacy of that information and therefore the government can gather it up without any constitutional issue whatsoever. It is not a search – there is no warrant, probable cause, reasonable suspicion, or even any reasonableness needed. It is not an intrusion on your privacy. That was a profoundly wrong decision that has led to the present situation, and it needs to be changed.

Robert O’Harrow:

Many of our laws do not contemplate the result of taking disparate pieces of data or records, putting them together, and then making them searchable by algorithms. There is a qualitative change in the information because it tells us things that would not have been known had they not been put together.

Prof. Burt Neuborne:

Professor Stone’s distinction between government and private corporations in respect to the dangers this information creates does not strike me as necessarily true in the current world. He is, of course, right that the Constitution gov-

erns the public sector and not the private, and that there is therefore a Fourth Amendment privacy interest in one and an inchoate set of values in the other. But it would be a mistake to think we should be zeroing in on government abuse and ignoring the enormous prospect of private power, especially when we have to answer Ms. Caproni’s very real question: Why should the government have less access to information than *The Washington Post*? Why should the government somehow be put at a disadvantage in carrying out its investigative responsibilities when these private databases are available to search for a fee? The real question is, should we be thinking about how to deal with the assembly of these databases? Once the information is there, it will be used.

We have discussed two values underlying the reason we care about privacy, which I still think is the central question we should be focusing on. First, we are worried about abuse of the information and, in Prof. Stone’s formulation, the special capacity for abuse that rests in the government because of its monopoly on force.

Second, I have always thought that the real reason we care about privacy, and the real reason we care about abuse, is because people do not know whether information is being gathered about them. This ignorance creates a climate that is inconsistent with the kind of spontaneity and autonomy needed for a vigorous free society. The *feeling* that we are being watched, whether or not we actually are, creates a deterrence on non-conventional behavior for which our culture will eventually pay a price. How do you keep people spontaneous and open in a world in which everybody is afraid that everyone else is going to know all that they are doing and saying?

EXCERPTS FROM THE QUESTION AND ANSWER SESSION

Lawrence Wright (*from the audience*):

I am troubled by the example of the national security letters. It does demonstrate the FBI self-correcting by examining its own behavior. In the process of looking at one tenth of the letters, though, it found more than a thousand violations. That seems to be a dramatic example of the government's inclination for overreaching its mandate. Unless I am mistaken, there has been no statement showing that any terrorist plot has been disrupted by the exercise of these NSLs. Ms. Caproni, could you please address these concerns?

Valerie Caproni:

Saying that there is nothing showing that an NSL has ever disrupted a terrorist plot is like saying no grand jury subpoena can ever be shown to have solved a crime. An NSL is a tool to gather the basic building blocks of an investigation. It is very difficult, in any given case, to say that a particular telephone or bank record led to the disruption of a plot. Investigations are far more complicated than that.

I can guarantee that NSLs were used as part of the investigation in any of our substantial terrorism cases that have been brought, just as grand jury subpoenas are used as part of the investigation in every large criminal case. So I have always thought that to be an unfair criticism relative to NSLs.

In regard to abuse, the inspector general's office found that there was no intentional abuse by any FBI agent. Second, they found no indication of NSLs being used to gather information that was not relevant to an investigation. That being said, we clearly fell down on our internal controls. I wish I could say that were not true, but it is. We had a substantial internal control problem that we did not detect. It was a problem of a unit getting out of control and being sloppy in how they got phone records. This was all a

phone record problem. It was not a bank record problem, which would be far more intrusive.

I wish we could say we did better. We certainly will do better in the future. But I think the critical elements are that it was not intentional misconduct and that the error rate you mentioned was the gross potential error rate. We slice that down to the real error rate. The inspector general was counting things such as mis-citing the statute under which we obtained a particular NSL. That is not something we should do, it is sloppy and unacceptable, but it is not a violation of rights. When you get down to the real violations, they were very few. There were too many, and we have tightened up training and internal controls, but there was no indication of intentional misconduct, which is what we should be most concerned about.

Prof. Geoffrey Stone:

The distinction between intentional and unintentional errors is not unimportant – intentional misconduct is obviously worse – but a large part of the concern is about carelessness and a lack of respect for the competing interests (in this case, privacy) that lead to it. That the violations were errors rather than intentional misconduct is relevant, but one should not therefore slough them aside as though they are not critical. In a society that allows the government to act in sensitive areas, you want an extremely high degree of care and attention to detail and accuracy. That is important whether you are dealing with free speech, privacy, or cruel and unusual punishment. You want to make sure the government knows what it is doing, does it carefully, and does it exactly according to the letter.

Valerie Caproni:

I don't disagree. There is no question that care is important. But I think everyone will draw a distinction, both viscerally and intellectually, between an agent who makes a typo in an NSL, thereby getting the wrong phone records, and someone who sets out to use a national security

tool to gather information on political enemies. The latter is totally unacceptable. Regarding the former, unfortunately, we just have to recognize that we are humans and humans make mistakes. The key is to detect the mistakes so that if we get the wrong person's records we don't do anything with them – we give them back, destroy them, get rid of them. That is where we are focusing our attention.

Prof. Katherine Strandburg

(from the audience):

I think it is absolutely correct that we should stop thinking about the surveillance issue as primarily about privacy, or perhaps even as primarily about autonomy. One example I am writing about is that, from a privacy perspective, we think about information that does not contain the content of communications as being of minimal concern. Traffic data is an example. All of our laws treat such information as a minimal concern, including the Fourth Amendment law that Prof. Stone was talking about.

When you put all of that information together and use different analytic techniques to look at it, though, you can get the equivalent of association membership lists. We have long-standing First Amendment law that strongly regulates the government's ability to ask for such lists. The reason for that is not about individual privacy – association membership is never private – but rather about larger social values.

The privacy perspective seems to focus on average people. When we think about things from a First Amendment perspective, we realize that the reason we have the First Amendment is not so much to protect average people as it is to protect our access, as a society, to non-mainstream ideas and political views. So I strongly agree that we need to expand our view of what surveillance is about beyond the perspective of individual privacy, and maybe even beyond the perspective of autonomy.

Question *(from the audience):*

Why do the private, corporate databases that we have been talking about exist? If they might be dangerous and bad, who makes that determination, the American people or the government?

Robert O'Harrow:

The basic answer is that they exist because we want them to. We as individuals love the conveniences, discounts, cell phones, banking, and all the rest. What these businesses do is collect records, pull them together, and ship off information. When we want to buy something, get credit, or have targeted mail sent to us, they look at our profiles and make choices. That is the service these companies were initially created to provide. In many cases, they are now becoming part of the security-industrial complex. They are providing conveniences and discounts that are banal at some level, but the information they collect is also being reused in different ways, including for private investigations, law enforcement, and national security.

Prof. Burt Neuborne:

They are private companies who gather the information absolutely legally because it is out there and because it is technologically possible to do so. There is a market for it. The information is available. The question is what we do with it.

CITIZENS SURVEILLED: FISA, The Patriot Act, and Today's Telecommunications

Panelists:

Bryan Cunningham, Barton Gellman,
Prof. Stephen Schulhofer

Moderator:

Prof. Matthew Waxman

Prof. Matthew Waxman:

The topic of this panel is surveillance of citizens and the major pieces of legislation that regulate it. We will particularly be discussing the Patriot Act, which was passed soon after 9/11 and expanded the government's law enforcement and investigatory powers in this regard, and the Foreign Intelligence Surveillance Act, which regulates the government's eavesdropping on domestic electronic communications. I would like for us to talk both about the legislation itself and the process of legislating in this area.

This is a fascinating and important topic for a few reasons. First, as Prof. Stone mentioned earlier, surveillance is a critical counterterrorism tool. Second, the information and communications technology that is the subject of this regulation is quickly changing and expanding. Third, we as Americans and our body of law care very much about privacy of the type discussed in the earlier panel.

I emphasize the word "American" because there is something unique in the way that we care about certain privacy rights that differs from how other democracies with similar legal

traditions regulate and care about them. In this regard, it is not so surprising that the Bush administration and Congress have been criticized for the way that they have conducted electronic surveillance since 9/11 and the way that they have legislated on it.

Bryan Cunningham:

Many of the people who are intensely interested in these issues refer to the 1970s as the starting point of discussion. There were many abuses of civil liberties in the long period after World War Two that I would differentiate from what is going on in the wake of 9/11. Congress took a number of steps after the Nixon administration to provide new and unprecedented regulation of the president's constitutional power to collect and use intelligence information both inside the United States and abroad. For the first time in our history, Congress and the president began to

regulate significantly the activities involved in foreign intelligence surveillance.

Congressional oversight from the inception of the CIA until the 1970s was essentially "don't ask, don't tell." Congress did not want to know how things were done and presidents of both parties did not want to tell them. But in the wake of Watergate and a number of other

scandals, including true domestic spying, Congress decided to start regulating that power, largely with the cooperation of Presidents Ford and Carter, and even President Reagan. President Reagan signed the executive order on



“The idea that the government should have fewer powers to prevent the next terrorist attack than it has in deadbeat dad cases, drug cases, and HHS cases strikes me as bizarre.”

Bryan Cunningham



Prof. Stephen Schulhofer, Prof. Matthew Waxman, Barton Gellman, and Bryan Cunningham. *Photo by Dan Creighton.*

regulating intelligence activities that is, with some but not much modification, still enforced today.

But the government has been surveilling for foreign intelligence purposes ever since the birth of the country. For the first two centuries, the courts consistently said that the president has plenary authority in the conduct of foreign affairs. Justice Sandra Day O'Connor in the 1980s said that the conduct of foreign intelligence collection operations lies at the “core” of the inherent executive power to conduct foreign affairs and defend the country. The relevant laws that were passed in the 1970s, including the Foreign Intelligence Surveillance Act, the Privacy Act, and others, were enacted against that backdrop. They were passed with the cooperation of presidents, but always with the caveat – sometimes spoken and sometimes written in internal legal opinions – that Congress could not constitutionally impair or impede the president’s power to collect foreign intelligence; that any law purporting to do so would itself be unconstitutional. President Clinton, among others, was advised by his Office of Legal Counsel that he was not only free to ignore such a law

but had something close to a duty to do so. So when we think about the compromises and balances struck in the 1970s it is important to think about them in historical context.

We should also bear in mind the crucial goals that Congress and the presidents were trying to balance during that time. The Foreign Intelligence Surveillance Act (or “FISA”) was essentially a bargain designed to balance the issues of civil liberties and privacy versus the president’s responsibility to protect the country. The framework was

an attempt to ensure, by and large, that overseas collection for foreign intelligence purposes is done *without* court involvement, while such collection done inside the United States is done *with* court involvement. It was based on two factors: personhood (whether or not someone is a U.S. person, a citizen, or permanent resident alien) and location (whether the collection was to be done inside or outside the United States). Those factors, in my view at least, were proxies for the real issue, which was balancing individual liberties against the duty to protect the country from attack.

Because of changes in technology and in the nature of our enemies, those two priorities can no longer be sufficiently balanced by the means that Congress decided on in 1978. It has become almost impossible in many cases to know in real time whether a person you intend to collect electronic surveillance against is located overseas or in the United States and whether or not they are a U.S. person. Similarly, laws like the Privacy Act were based on the notion that the government would keep paper files. One of the protections that the Privacy Act provided is that paper files that include infor-

mation about Americans could not be deliberately pulled together, at least without public notice. Now, of course, the vast majority of information is electronic, and therefore computer searchable. So how do you adapt the goals of such legislation to today's technology?

This is a crucial question that the government is grappling with. Reforms of FISA are currently being debated, and all of the issues in that law, technical and otherwise, are hopefully being looked at with a view to protecting the same interests but in a way that makes sense today.

Prof. Matthew Waxman:

What do you see as the next big issue or set of issues in this area about which Congress may want to legislate?

Bryan Cunningham:

Over the next five years, many of the issues involving individual privacy will revolve around whether or not we believe that our privacy is significantly infringed when machines rather than people look at information. My prediction is that many of the solutions will involve having computers triage data before human beings ever get to look at it. Data that is not relevant to a legitimate national security interest would either be not collected in the first place or be quickly destroyed.

People have different views about that. Some feel absolutely that their privacy would be violated by a government computer picking things out. Others are indifferent, as long as the information is not kept and the collection cannot infringe on their liberty, their right to travel, or their financial freedom.

Prof. Stephen Schulhofer:

When we think about privacy, we think about it primarily as a question of access to information. As a result of 9/11, the government now has far more access to far more information. I would like to mention four examples out of many.

First, the government can now eavesdrop on international calls into and out of the United States without a warrant and without any individual suspicion. The same power extends to international e-mail, including the e-mail of U.S. citizens living abroad. A second change affects domestic e-mail. Contrary to many claims, the government has not gained new power to access the content of domestic e-mail but there is greater access to what is called "envelope information." That includes not only the addresses of the sender and the recipient, but also Internet users' search terms and the identities of Web sites they visit.

The government can now get this information even when the person affected is not suspected of any criminal activity. As the prerequisite, the government must certify that the information is "relevant to an ongoing investigation." That is the statutory phrase. A less-complicated way of saying the same thing is that the FBI has to certify that it is not acting in bad faith; it has to self-certify that it is acting in

good faith. That is the whole requirement.

A third change involves so-called "sneak and peek" searches, which are clandestine entries into homes and offices to seize property, copy files, or plant listening devices. The FBI now has much greater power to conduct these kinds of secret searches. Regarding telephone and e-mail, we are talking about the surveillance of literally millions of messages. Secret



“Since 9/11, we have seen a dramatic reduction, and in some cases the complete elimination, of meaningful oversight across the entire range of intelligence-gathering issues.”

Prof. Stephen Schulhofer

searches are much less frequent but when they happen they can involve massive invasions of privacy. When the FBI misidentified Brandon Mayfield's fingerprints at the site of the Madrid train bombings, they conducted repeated secret searches of his family home in Oregon. They bugged his bedroom. They also conducted secret searches of the files in his law office.

The fourth change on my incomplete list is enhanced access to documents and records. Before 9/11, most records were accessible only through the grand jury subpoena process. But the Patriot Act gave the FBI much easier access to the most private sorts of records, such as medical records, book store purchases, membership lists, and the contributor lists of political and religious groups, which would include churches and mosques.

Many people assume that these invasions of privacy prove an egregious power grab. I do not make that assumption. Even without the 9/11 attacks, there was nothing sacrosanct about the pre-9/11 baseline. There certainly could be good reasons to reconsider any of the rules that we had in place before. But I think it is important to acknowledge that these are big changes in the government's power to access and amass private information. Powers like these have led to enormous abuses in the past, as Bryan Cunningham mentioned.

The threat is not solely a threat to privacy in the traditional sense – the sense that what I read or what I say to my friend is none of anyone else's business. That kind of privacy is what I would call Fourth Amendment privacy and is obviously important. The threat to privacy also has a political dimension, essentially a First Amendment dimension, that Prof. Strandburg



“Over the next five years, many of the issues will revolve around whether or not we believe that our privacy is significantly infringed when machines rather than people look at information.”

Bryan Cunningham

talked about earlier.

There is also an enormous amount of personal information in the hands of the private sector.

The private sector uses it primarily to sell things. There can be problems in this area but they rarely threaten the foundations of our society. Information in the hands of the government is very different; although it can be used in the public interest, it can also be abused.

Throughout history, the government has used private information to chill the free exercise of religion, to stifle political protest, and to intimidate or blackmail political opponents. So government access to information is dangerous. It is playing with fire. Lighting fires is sometimes necessary, but must be done carefully, not automatically and on increasing scale whenever somebody thinks a fire might do some good. We have to look closely at the need for these enhanced powers and ask whether there are better ways to accomplish the same goals. In some of these areas, I think there are much better ways.

I would also like to mention some aspects of privacy that go beyond the familiar concerns about access to information. I have not yet mentioned the Foreign Intelligence Surveillance Act. Contrary to conventional wisdom, the prerequisites for surveillance under FISA as to U.S. citizens are not much different from the prerequisites for surveillance in ordinary criminal investigations. Those prerequisites were not much changed by the Patriot Act. Nonetheless I think that FISA is a big deal. In the case of U.S. citizens, the main difference between FISA and ordinary criminal investigations is not in the prerequisites but rather in the mechanisms of oversight. Oversight mechanisms are very

strong in the context of ordinary criminal investigation and surveillance. They are very weak under FISA. Although the post-9/11 changes did not reduce the prerequisites for surveillance of U.S. citizens, they did dramatically reduce accountability and oversight.

When we think about the right to privacy and how it is changing, we need to think not only about access but also about the safeguards that provide accountability for the way the access powers are used. We have seen an erosion of the norms that were in place before 9/11 in respect to both access and accountability, but there is one major difference between them.

There is some logic to the idea that new threats may justify more access but no logic at all to the idea that they justify the dismantling of oversight. To the contrary, accountability becomes more important, not less, as government acquires more power to accumulate information.

Since 9/11, we have seen a dramatic reduction, and in some cases the complete elimination, of meaningful oversight across the entire range of intelligence-gathering issues. This damages our Fourth Amendment privacy and aggravates the damage to our First Amendment privacy that shelters dissidents and political opponents from the abuse of power. This reduction of accountability is not justified by any supposed need to shift the balance between liberty and security.

I have so far talked about privacy in terms of access and accountability. There is a third dimension that has changed since 9/11, regarding our rule-of-law culture. The issues that I have talked about raise questions about basic values. Reasonable people can certainly differ about how the answers should be framed. For that reason, the judgments should be made

openly, through public discussion and deliberation in Congress. There is no reason why they should be made solely by the president and a tightly controlled inner circle of advisors. This



Bryan Cunningham. *Photo by Dan Creighton.*

administration has had great success in convincing much of the public that because we are at war it is legitimate, and indeed essential, for the president to make these decisions unilaterally and in secret, even when the new measures violate pre-existing statutes.

What should concern us is not only whether the president's position is legally correct, which it is not, but also the degree to which much of the public has come to accept this position regardless of its legality. We see evidence of this not only in the reluctance of the Democrats in Congress to push back but also in the amazing argument being made that if telecommunications companies violated the law (which we do not know yet) then they should be given retroactive immunity from damage suits because they complied with government requests to ignore the law.

Protection for our privacy depends on something that we took for granted before 9/11, and that is simply the rule of law. The Bush administration has announced that previous laws are out of date – “quaint” was one of the terms used – and has then proceeded to flout those laws

without any apologies. Worse, and something that may outlive the Bush administration, is the idea that this approach is necessary for our security and that Americans will die if we insist on making and changing the laws in the ordinary way. Fear has led many Americans to willingly surrender not only their privacy but also their commitment to self-government and the rule of law. The erosion of e-mail privacy is worrisome but this last development is really scary.

Barton Gellman:

At a conference in October 2007, Donald Kerr, the principal deputy director of national intelligence, said that “protecting anonymity isn’t a fight that can be won.” He went on to say that “privacy is a system of laws, rules, and customs with an infrastructure of inspectors general, oversight committees, and privacy boards on which our intelligence community commitment is based and measured.”

That is not what privacy is. Privacy at some elemental, gut level is the ability to say, “Mind your own business.” It is the ability to control the degree to which we are transparent to others and whether there is any important respect in which we have that power against those who want know something about us. In this case we are talking about governments.

People in the intelligence business and the private-sector information business tend to say, “Oh you poor, silly man. Don’t you understand that privacy is gone? Just get over it. Technology and our current social norms overtook that a long time ago.” There is quite a bit of truth to that, but it is a result of laws, directives, operational procedures, and systemic norms that we have created. Those factors not only can change but have changed quite sub-

stantially in recent years. The question that we need to debate as a society is whether they need to be changed some more.

I would like to describe the arc of change regarding the national security letters that were discussed earlier. Because of the reforms in the 1970s that Bryan discussed, legislation such as the Electronic Communications Privacy Act, the Bank Secrecy Act, and the Fair Credit Reporting Act said, to state it broadly, that information could not be collected; that it was private. Exceptions arose fairly quickly, including national security letters. For a few decades, NSLs allowed the government to get access to private records if they had a specific and articulable reason to believe that those records belonged to a terrorist or a spy. At first it was limited to spies; terrorists were added later.

The Patriot Act eliminated any need to have a specific or articulable reason and any need to

believe that the records belong to the subject of the investigation. The standard now is that the information is either “sought for” or “relevant to” an authorized investigation to protect the country against spies or terrorists, depending on the statute. For example, the government may be inter-

ested not only in an individual’s phone records but also the records of everyone he has called, in order to find links. The threshold level of relevance required is extraordinarily low.

The government has assured us that it takes privacy seriously and that these tools are used sparingly and for good reason. But the March 2007 inspector general’s report, said, among other things, that the supervisors and particularly the field counsel in FBI field offices were generally reluctant or afraid to question either the relevance or the factual predicate for NSL requests. As a result, banks and phone companies receive letters asking for all of a person’s



**“Privacy at some elemental,
gut level is the ability to say,
‘Mind your own business.’”**

Barton Gellman

records and are told that they can never tell anyone that the request was made.

That is one set of changes. The attorney general guidelines for national security investigations reflect another set of changes made after 9/11. The guidelines used to say that information pertaining to a U.S. person that is deemed not relevant at the close of an FBI investigation shall be discarded. Now they say



Prof. Stephen Schulhofer. *Photo by Dan Creighton.*

that the information shall be retained. That's forever. They have swept up an enormous amount of information that they have deemed not to be relevant to a particular investigation. It is going to stay in a government databank because it might come in handy later. And it might come in handy, it could be very important in connecting dots at some future point.

The guidelines used to call for a variety of checks and restraints on sharing information that was safeguarded in one protected place. Now, in the post-9/11 world, where we are interested in breaking down walls, the guidelines carry a strong presumption that it shall be shared. The president signed an executive order extending that sharing to state, local, and tribal law enforcement authorities, and appropriate "private sector entities," a term which has not been publicly defined. So the government has the ability to sweep in more information, to

retain it, and to share it more broadly. There are very good motives – to stop the country from being attacked – but the changes are substantial. I think that the costs and benefits have not been well debated because most people do not understand the extent to which it has happened.

In writing a story on national security letters for *The Washington Post* which ran in November 2005, I talked to senior FBI and

Justice Department officials. One of the arguments made by Joseph Billy, the FBI's assistant director in charge of counterterrorism, was that people about whom information has been collected could feel that they've done nothing to be concerned about. That argument is often paired with the observation, made accurately by Valerie Caproni earlier in today's discussion, that there has been no showing that anybody has abused this information, in the narrow sense of blackmailing their political enemies, spying on their former spouses, or pulling information from these databases for improper reasons. But the question is whether the routine collection and review of information for very broad law enforcement purposes is something Americans are prepared indefinitely to accept.

Personally, I have many things to hide. One set of those things includes who I talk to during my reporting and how I get information from confidential sources. Of course, what someone has to hide depends on whom he is hiding it from: I do not want my colleagues to know my salary, I do not want my employer to know that I am negotiating to leave my job, and I do not want one friend to know that I am skipping his wedding to go to another friend's party. There are many things we want to keep to ourselves. The idea that we have nothing to hide, that we should not mind this enormous accumulation of data about us, is naïve.

The theories of link analysis and datamining under which the government might want to use some of this material, to the extent that it becomes able, depends on the ability to find meaningful connections among the many terabytes of data that the intelligence community collects daily through many methods. In weighing whether the effort is efficacious, we should consider a study done for the since-abandoned Total Information Awareness Program. A consultant named Mary DeRosa has spoken about the degrees of separation among the September 11th hijackers. Khalid Almihdhar was on a government watch list, making him a known suspect. Mohammed Atta was one degree of separation away from Almihdhar because they used the same contact address. Wail Alshehri, another hijacker, was two degrees away from Almihdhar because he and Atta shared a telephone number. Satam M.A. al Suqami and Alshehri shared a post office box, so al Suqami was three degrees away from someone on the watch list.

All this sounds like it could very helpful to intelligence analysts but you have to consider that everyone has one degree of separation with hundreds, and almost certainly thousands, of other people: alumni of the same high school, people who live in the same high-rise apartment building, people who once took a flight together, and so on. There will probably tens of thousands of such connections. When you get into two degrees of separation, there will be hundreds of thousands or millions. With three degrees, everybody is fairly quickly linked, creating an argument for collecting and retaining almost everything about almost everyone.

As a thought experiment, it might be valuable in preventing or solving crimes, preventing terrorism, or preventing espionage if every one of us, once we turn 18, were required to wear a watch that would record everything we say and everywhere we go. If we do not want to go that far, where do we want to draw the line?

Prof. Matthew Waxman:

When we think about checks on executive power, we usually consider checks between branches of government. The press also serves such a function. How you see the press's role in that regard, especially in respect to executive national security powers? As a related matter, I assume that journalists rely heavily on electronic communications to do their jobs. Do the types of powers that the executive has asserted, either with or without a congressional blessing, affect your profession and its ability to be effective?

Barton Gellman:

My personal view is that the press has no formal institutional entitlement. Functionally, public exposure and discussion are what is important. In order to hold the government accountable, one has to know, in broad terms, what it is doing.

The importance of privacy is well-understood by the government for its own purposes. In terms of its deliberations, in terms of who is advising the energy task force, and in terms of a long list of information that Congress would like in exercising oversight responsibilities, the executive branch is prepared to say that it would be difficult to get full, unvarnished opinions from anyone who knows that his or her advice will be publicly aired. This is all in the pursuit of the public business. Government officials have no legitimate right to personal privacy in their public capacities. That is, the privacy interest is not theirs as individuals. Any valid argument here is about the best way to serve the public interest. I agree that there is a plausible argument, and sometimes rather an important one, that deliberations require some privacy. On the other hand, choosing their elected officials and holding them to account clearly require people to understand something about what the government is doing. Since Congress and the courts, for many complicated reasons, are sometimes disinclined to or ineffective at

extracting that information and making it public, reporters fill that role.

We have to have confidential sources because in some cases people will lose their jobs or face other sorts of retribution for talking to us. Cell phones and e-mail are very convenient, and I do not think any of us have figured out an effective way to avoid any exposure.

Sources of mine have told me they had been interviewed by leak investigators. Based on the questions they were asked, they were fairly confident that their own phone records had been obtained. They gave me a heads-up about it because it would mean that my records might have been obtained or that, at least where the records crossed, my contacts might be known. It is a conundrum. The boundary preventing intrusion into the reportorial process, which has evolved in the several decades since Watergate, is shifting in a way that is not particularly helpful to public debate.

Prof. Matthew Waxman:

Mr. Cunningham, do you think we have found the right balance between secrecy and transparency? Is there a perhaps a better way to strike it?

Bryan Cunningham:

I do not think that we can strike the right balance for all time. This point underlies my earlier remarks about FISA. It depends. For 225 years, the courts have said that the balance between the First Amendment and the Fourth Amendment against the government's security powers will change over time based on the circumstances.

It seems to me there is something fundamentally anti-democratic about the notion that the president of the United States, who is elect-



“Protection for our privacy depends on something we took for granted before 9/11, and this is simply the rule of law.”

Prof. Stephen Schulhofer

ed by the people, and the Congress of the United States, which is also elected by the people, approve and oversee top-secret intelligence programs, and the editor in chief or the publisher of *The Washington Post* or *The New York Times* can decide to destroy those programs by revealing their existence. There are times

when that would be probably beneficial. There is a special place in our country and in our constitutional law for journalism, but I do not think that it can go as far as to give one person, effectively, a veto over decisions made by the politically elected branches of government.

Barton Gellman:

The press is not qualified to make decisions about how best to protect the United States from attack and is not entrusted by the people to do so. The president is disqualified as a democratic, philosophical, and constitutional matter from deciding what the people need to know about him in order to evaluate his performance or judge whether he ought to be re-elected.

There are intersecting disqualifications and sometimes a flat conflict of interest between national security secrecy and democratic self-government, both of which have strong foundations in the Preamble of the Constitution. “We the people” are supposed to make the decisions, and there are fundamental interests we are trying to protect, among them the common defense.

Prof. Matthew Waxman:

Prof. Schulhofer, could you please give us a sense of how you would reform the system? How, for example, would you address FISA?

Prof. Stephen Schulhofer:

We need to focus on accountability. Although we have to be aware of the need for secrecy under many circumstances, there are steps that could provide for more effective accountability structures. They include reporting to congressional committees about the nature of the programs, on a confidential basis when necessary. That is one thing we could do.

The 9/11 Commission recommended the creation of a civil liberties oversight board within the executive branch. That is a promising idea, although it is a bit different from the way we usually think about accountability because it is internal rather than between branches. It creates structures within the executive branch to provide a degree of independent checks and balances. The inspectors general of the various departments are another example. The idea is anathema to those who believe in the unitary executive and the power of the president to control the executive branch without any independent internal oversight. I do not think their case has been made. With an independent check within the executive branch, many of the hesitations about classified information and other matters could be overcome.

A proposal for an oversight board such as the one recommended by the 9/11 Commission was added to a larger Senate bill in a way that made it veto-proof. However, the devil is in the details. The Senate passed a version that would have created a full-time chairman and vice chairman who could only be removed for cause. It would have given them subpoena powers

within the executive branch and would have required them to hold security clearances. But the conference report removed all of the provisions that gave the oversight board independence and the ability to actually investigate anything. So we do have a civil liberties oversight board but it has no structural independence or capability.

There are many things to be said in reference to FISA. One particularly salient issue is the absence of notice at any point. In criminal investigations, people are notified that they have

been a target of surveillance 90 days after the surveillance ends. Without notice of a FISA search, there is no possibility of an external check to determine whether or not the rules were followed. FISA has an interesting provision for civil liability against any government agent or private company that violates the statute's rules, but how could anyone sue if they are never notified that they were a target of an investigation? They aren't and so they can't. People who are later prosecuted get a limited form of notice, but we should be even more concerned about

those people who aren't. Those are the cases in which there is likely to be overreaching or abuse – the investigation of people who shouldn't have been investigated. FISA is structured in such a way that only the legitimate targets are ever notified. People who shouldn't have been targets never find out that they were subjected to surveillance. There is no structure in place to keep the system operating within its own rules.

There is a legitimate and important conversation to be had about whether we are now facing a different threat environment than we were before and whether the government needs new powers as a result. But even if new powers are



Prof. Matthew Waxman. *Photo by Dan Creighton.*

needed, it is quite different to give the government those powers without any oversight.

EXCERPTS FROM THE QUESTION AND ANSWER SESSION:

Valerie Caproni (*from the audience*):

Mr. Gellman, you seem to be critical of the requirements for national security letters, which were changed from specific and articulable facts to believe that a person is a terrorist or a spy to mere relevance. Why should the standard for gathering this information in a national security context, where arguably the risk is much greater, be different than in a criminal context, where the standard for a grand jury subpoena is relevance?

As a hypothetical, the British security services after the London subway bombings gave us information on contacts between the bombers and people in the United States. Was it appropriate to use national security letters to gather the phone records of people who were in direct contact with the bombers? If so, how could we have done that under the pre-9/11 standard of specific and articulable facts? We did not know whether people in contact with the bombers were terrorists, we knew simply that they were in contact with terrorists. So it was relevant, but we did not have specific and articulable facts.

Barton Gellman:

My point was not to say what the standards should be but rather to point out, in light of the argument that privacy is already extinct and we should get over it, that this state of affairs depends on current laws and practices. If the government, or a data aggregator like Nexis, were not allowed to collect and store my personal data, then it would stay private. Privacy has ebbed and flowed with changes in laws, standards, practices, and so on. Although I hesitate to debate the law with a lawyer, I would note that there are differences between grand

juries and NSL investigations. There is at least some level of supervision or accountability involved in asking a grand jury to issue a subpoena. A subpoena is not automatically and permanently secret, so the recipient and subject of a subpoena are not automatically and permanently barred from discussing the fact that the records were obtained.

Bryan Cunningham:

Ms. Caproni's question brings up an important and broader issue. When I served in the Clinton administration, I not only served in the CIA but also as a special assistant U.S. attorney prosecuting drug cases. I went to federal judges and got dozens of sneak and peek warrants. I got roving wiretap orders that allowed me to surveil any communication device that a particular suspect used. Such orders were not available under FISA for national security cases before the Patriot Act, nor were sneak and peek warrants.

The Drug Enforcement Agency has the authority to issue administrative subpoenas, which are similar to national security letters. The Department of Health and Human Services has administrative subpoena authority to get healthcare records without judicial involvement in the first instance. The idea that the government should have fewer powers to prevent the next terrorist attack than it has in deadbeat dad cases, drug cases, and HHS cases strikes me as bizarre. Furthermore, it seems to me that a person's liberty interest would be far more affected by a criminal subpoena or a criminal wiretap, in which case they may well be on their way to jail, than by a national security letter. I am not trying to say that a war on terror justifies anything that the government may want to do, but in debating these questions we have to consider the government's powers in many more routine and less existentially threatening situations.

Prof. Stephen Schulhofer:

I would like to respond, because there are some distinctions that are worth noting. As Mr. Cunningham says, prosecutors can get so-called “sneak and peek” warrants (officially referred to as “delayed notice” warrants). With sneak and peeks in the domestic law enforcement context, the FBI, DEA, or other law enforcement agency sneaks in and conducts its search rather than knocking on the door of the premises with a copy of the warrant. But the victim is notified within a court-specified period of time. It used to be seven days; now it is about 30. That has always been part of our law and I think it is appropriate.

In the FISA context, there is *no* notice. This is an important difference in terms of the risk of abuse and the need for a system of accountability. The absence of notice is automatic. Sneak and peeks under FISA were available before the Patriot Act. That is one of the reasons why I think criticisms of the Patriot Act are exaggerated. Sneak and peek power without notice was already available in foreign intelligence investigations. The change introduced by the Patriot Act allows for no-notice sneak and peeks under FISA when criminal prosecution is their primary purpose. In other words, the change did not create sneak and peek power but permits prosecutors to avoid ever giving any notice to the target. That is something I think we should worry about.

REINS OF POWER: From Wall Street to Washington, D.C. and the Global Information Network

Panelists:

Jeff Jonas, Vivian Maese, Declan McCullagh

Moderator:

Karen J. Greenberg



Karen J. Greenberg and Declan McCullagh. *Photo by Dan Creighton.*

Karen J. Greenberg:

This discussion will introduce some new twists to this morning's policy debates. I would like to find out what the panelists think the future holds in store for us and whether there is anything, in fact, that we can do about it.

Vivian Maese:

I would like to preface my remarks by noting that my comments will be from my personal observations and not reflective of any of my employers. Because I have been concerned about and involved in these issues, my son may be the only teenager without a page on MySpace or Facebook. I am aware of the benefits as well as of the burdens of ubiquitous technology. I think there is a cultural divide about whether or not we want privacy legislation. The

issue can be seen generationally. Those of us who are a little younger feel comfortable advertising everything about themselves to the world. Older people are more accustomed to modesty and privacy. It is an interesting cultural division that I think stems from the difference between growing up with technology and growing up without it and incorporating it into your life later.

While we have been given technological tools, we have not been educated about the ways they can be used. The market for technology has grown up in a fragmented way. We haven't been asked whether we want to give away our personal information so that companies can charge for data about us individually or in the aggregate. There is nothing stopping people from creating such business models. In the late 1990s,

when technology started to become increasingly ubiquitous, there was a great movement towards privacy legislation. We were making some progress. Then, after 9/11, we essentially told the government, "Here, take all of our information. Just keep us safe."

We are now past that stage and trying to figure out where we want to be. Culturally, we are a bit torn. We want certain information to keep us safe. On the other hand, as Robert O'Harrow indicated earlier, we have the advantage of the market in information being fragmented. Although there is some conversation about automating health records, and bank records are certainly online (many of which may be in other parts of the world at this point), it is all individual. Assimilating the information is a time-consuming process. But, to borrow

Mr. O’Harrow’s analogy, the picture becomes clearer as technology advances and as databases start to be collected, consolidated, and collated. That is a sacrifice of what we could call our privacy. In some cultures, people believe that when they are photographed pieces of their spirits are taken. When we reach a point at which there is such transparency about who we are, has something actually been taken from us? It would then be too late to create the laws that we would need to protect us from getting there.

Right now, we as a culture need to figure out where we want to be on this topic. We have to think about legislation that establishes the standard we want. We must also start to think practically about globalization. We are in a global economy, without question. Corporations led the way a couple of decades ago and we are now seeing it now in academia and other institutions. We need to think about ourselves not only as members of this society and this culture, but also how we fit into the rest of the world.

The legislation has to be transparent about the uses of information. We know our banks are using the information we give them, for example. But there are downstream uses that none of us can foresee and that need to be controlled, or at least disclosed. We resign ourselves to surrendering our privacy because we cannot really effect any change. Who are we, individually, against these monolithic corporations that have collected all of this information? The banks’ privacy policies are given in very fine print on our monthly account statements. We do not usually understand them because they have been written in a way that obfuscates what is actually going on. But what are our choices? What control do we really have? Moving to other banks



“Legislation has to be very transparent about the uses of information. . . . There are downstream uses that none of us can foresee and that need to be controlled, or at least disclosed.”

Vivian Maese

or companies would be very dislocating. So, the transparency of the uses will be important to the next generation of protections.

Many states, and New York City also, require people to be told if their information has been compromised. Notification is fine but there is no practical remedy. You can’t do anything about it but it is good to know.

Legislation also needs to address information security. Most businesses see compliance as an expense. Absent a compelling reason provided by legislation – either through penalties for lack of information security or through financial incentives such as tax rebates to invest in technology that would enhance it – most corporations would not willingly spend the money that would be required to protect the information.

Until we as a culture resolve these questions and cause a groundswell around them, we will not be able to enact the laws we need to protect us. Today’s conversation is a great start.

Karen J. Greenberg:

What are the regulations regarding the storage of electronic information? How long is it kept?

Vivian Maese:

It varies from place to place. Many record retention requirements are geared for a paper world. Compliance requires a lot of translation.

In the securities industry at least, e-mail almost never goes away. There are two conflicting priorities – transparency and disclosure on one side and privacy on the other. In the regulatory environment, and securities law is the one I am most familiar with, the rules for e-mail say that all communications about business as-such

must be kept. However, there is no way for software to distinguish e-mails about where to go for lunch, for example, from those about the details of a specific transaction. Most large organizations are stuck with having to save everything, and they do. The e-mails should be deleted after three years but they are generally not indexed appropriately. If there is any litigation, they must be retained for the duration of the litigation. They cannot be destroyed. So they stay around for a long time. Tax lawyers need documents around for at least a 12-year time horizon.

In some countries, retention is required for 15 or 20 years. Global organizations manage their obligations by finding the common denominator.

Jeff Jonas:

In the early 1990s, my company, Systems Research and Development, started deploying systems to help casinos detect potential security problems and preempt them from happening. Then the U.S. government became interested in my technology. I received some funding from In-Q-Tel, the venture capital arm of the CIA. This was prior to 9/11. The government's interest in my technology was to help find criminals within. Then, after 9/11, the technology started to be used for national security and counterterrorism. IBM acquired my company in January 2005.

For the last four or five years, my focus has been shifting. I am becoming more and more aware of technology's policy and privacy ramifications. I have become somewhat vocal in the area, publishing papers on topics such as the



“I know of at least one case in which the administrators of a watch list did not know the original source of the information on it. How could that not be arbitrary? If data is moving, it is important to know where it came from.”

Jeff Jonas

limited uses of datamining for counterterrorism. Today I am speaking on my own behalf rather than IBM's.

According to the American Civil Liberties Union's "Surveillance Society Clock," we stand at six minutes to midnight, with midnight representing total surveillance. I started thinking, could it really be six minutes? So, I came up with what I thought to be six plausible ticks, which I wrote a blog post about. The first one that I conceived of – although it could be any six ticks –

was the fact that every cell phone has a global positioning system. You cannot buy a cell phone without one. The next thing I thought about were radio frequency identification chips, which are little devices that can give a signature to anything. If you lose your glasses, for example, your cell phone can tell you where they are.

My conclusion was that a total surveillance society is not only inevitable and irreversible but also irresistible. As consumers, we are going to love finding out where the closest Starbucks is. This is going to lead to the kind of future I think we are heading towards. I think that we haven't seen anything yet. Ubiquitous sensors are coming fast, and it is because companies are competing. If one bank figures you out better than another bank, it wins. Businesses are trying to collect and take advantage of more data and instrument more things.

This suggests a future with a ton of data, and it will not be created by the government. It is going to be created commercially. The policy debate comes down to who gets to peek at the data, when, and with what oversight and accountability?

People frequently ask me where the information winds up after they give their names and birthdates to the phone companies, credit companies, and so on. Instead of answering the question repeatedly, I decided to write a blog post about it. My conclusion was that when a company collects a piece of data, they back it up: once a day for seven days, maybe back those up weekly for 52 weeks each year, and then annually. After that, they take the information from their production systems and put it in their data warehouses and in other things called



Vivian Maese and Jeff Jonas. *Photo by Dan Creighton.*

“data marts.” Both the data warehouses and the data marts are also backed up. The result is that after you give your name and date of birth to a company, there are almost never just 10 copies. There are almost certainly more than 100 copies, and in some cases more than 1,000, more than 10,000, or more than 100,000. I think there are some scenarios in which there are a million copies.

I spend much of my time now thinking about what we can be doing as technologists to prevent us from some day waking up in a bed that has already been made. One of these is the notion of immutable audit log. Peter Swire, the Clinton administration’s chief counselor on privacy, and I penned a paper on this subject published in February 2006 by the Markle

Foundation’s Task Force on National Security in the Information Age. The idea behind an immutable audit log is to record, in a tamper-resistant way, how somebody uses a system. Even if the people managing the system are corrupt, the log would provide evidence if it had been tampered with. The more non-transparent the system is, the more important it would be to have that kind of technology nearby.

I have spent some time working on anonymization. Such technologies help protect personal information in information-sharing environments. If a user needs to identify someone, they can find the original piece of data and make a request for it, but their doing so becomes a very observable event. Anonymization techniques will help reduce the risk of unintended disclosure.

I know of at least one case in which the administrators of a watch list did not know the original source of the information on it. How could that not be arbitrary? If data is moving, it is important know where it came from. That way, someone could

go back and correct the information if it turns out to be inaccurate. I refer to this as “tethering data.” It turns out that once you get more than two or three hops away from the source, tracing it back becomes very difficult and very expensive.

Karen J. Greenberg:

What are the realistic, discernable dangers presented by hackers?

Jeff Jonas:

The cost of identity theft and credit fraud is enormous. The smart actors are playing in low-signature space. They are not creating big events and stealing a hundred million dollars because they would be tracked down. They real-

ize that if they steal less than a certain amount – let’s say \$2,500 hypothetically – then they would be too low of a priority to be caught. As a result, they would do all of their work at \$2,455 in our example. What if somebody were to create an automated system that would do



Declan McCullagh. *Photo by Dan Creighton.*

low-signature attacks, but against 200,000 people simultaneously? That would cause a lack of confidence in financial systems and a rush to respond.

We should keep in mind that the pendulum invariably swings fairly far. If we do not think now about how to protect ourselves and create infrastructures that we like in advance, the response after something happens may not be what we would choose.

Declan McCullagh:

I would like to make two points, the first legal and the second technical. The first is about the growth since 9/11 not only of laws but of par-laws or metalaws. By that I mean laws that seek to restrict or regulate conduct that is already illegal. Instead of targeting the underlying crime, such laws regulate acts that normal citizens participate in everyday, in case there may be a few instances in which they are proximate to a crime. In addition to laws against blowing up subways, which was already a

crime, for example, we now limit taking photographs on the subways, a paracrime. In addition to banning bombs, we restrict the sale of chemicals that have innocent uses.

Such laws are not new. We have restrictions on the sale of lock picks, on marijuana possession, and on gun ownership. I am not saying that all of these laws are unreasonable but I bring them up for two reasons. First, I suspect the distance between crimes and paracrimes has widened over the last six years. Second, in evaluating whether a law is just or reasonable, it is useful to evaluate whether it addresses a crime or a paracrime.

In terms of technology, there is an argument that it has hurt privacy more than helped it. We have heard some examples earlier today. That argument does make some sense. But sometimes we dwell too much on the negative and not enough on the positive. Privacy is making at least a slight comeback through technology. One way is through encryption, which can protect both stored data that might be sought by a search warrant or other compulsory process and also data that is live in-transit, which is typically sought and intercepted with a Title III or similar wiretap order. A decade ago, using encryption was difficult, especially for stored data. But now, newer versions of Windows and all recent versions of Apple’s OSX operating system have built-in encryption. On my computer, I can turn it on by clicking “encrypt” and typing in a password. As long as you pick a password that is sufficiently strong and hard to guess (not your mother’s maiden name or your birthday, for example), you are theoretically secure against federal cryptanalysis attacks, at least as long as the theory of encryption we currently have is correct.

If you use a laptop to work from home, you

are probably using a virtual private network. That way, you have a secure connection. Your Internet service provider cannot see the contents of your communication, and neither can any FBI Carnivore DCS1000 box sniffing your ISP's network. Encryption is making its way into e-mail as well.

But encryption by itself is not enough. If an adversary can correlate who is talking to whom, that can be very useful information and sufficient to endanger the privacy of those involved.

Online anonymity was born from the cyberpunk movement in the early 1990s. It is has matured, although it still not quite perfect, through systems that can conceal your identity while you are browsing the Web. This is a powerful idea. Your privacy is now protected by these services rather than by federal laws that can be reinterpreted by the executive branch or by judges. It is protected through the immutable laws of mathematics.

This does create problems for law enforcement, and private litigants to a lesser extent. We are seeing a sort of counter-counterattack by law enforcement. In their investigation of Nicodemo Scarfo, whose federal prosecution in New Jersey I have written about, FBI agents armed with a

court order basically snuck into Scarfo's office late at night, planted a keylogger, recorded his encryption software passphrase, and were able to get the documents they wanted. More recently, federal agents, armed again with a court order, sent spyware called "CIPAV" (for "Computer & Internet Protocol Address Verifier") to a MySpace account associated with bomb threats at a high school in Washington State. That led to the identification of a student who pled guilty in July 2007.

Karen J. Greenberg:

Given today's conversation, what exactly do Google and other search engines represent, in terms of what is happening to us and our relationship to information being kept about us?

Vivian Maese:

The information is now fragmented. But when all of the pieces of information identifying your favorite color or where you like to vacation start coming together from your bank, the healthcare databases, and the companies you do business with, suddenly there is a robust picture of who you are. That subjects you, as an individual, to all of the prejudices there may be in the world about people with blue eyes, brown hair, or whatever attributes describe you.

Jeff Jonas:

All of the data within an organization constitute its perceptions and represent the limit of the organization's intelligence.


It is one matter for the organization to take advantage of the perceptions they already have because it is their own knowledge, but what about when they look over the fence? Should they be able to ingest the information in the phonebook on their shelf?

Should they be able to use Facebook, Google, LinkedIn and MySpace to figure out whether or not to offer you something? I think that question will be the focus of much of the debate.

Declan McCullagh:

I should preface my response by noting that my wife was recently hired by Google as product counsel, but my remarks are my own.

Search privacy is an important form of self-disclosure, because you can search for very sensitive information about yourself, including financial and medical matters. Two events



“A total surveillance society is not only inevitable and irreversible but also irresistible.”

Jeff Jonas

changed the way that people think about it. The first was in connection with the Justice Department's need for statistical information to buttress their support for the Child Online Protection Act in a litigation in the Eastern District of Pennsylvania. They tried to subpoena search terms, excerpts from Google's database, and other materials. They did not get what they wanted but it demonstrated to the public that the issue is important. The second formative event was AOL's disclosure of search records during the summer of 2006. The records were

anonymized but it was invasive nevertheless. This point is not limited to search engines. Many other types of Web sites have search bars in which people will enter sensitive information.

Most search engines use behavioral advertising. In other words, if you type "New York" in one search and the next day query "hotels," the search engine will know that you are looking for New York hotels. An easy way to protect yourself is to delete your cookies, which is an option in most modern Web browsers. That way search terms cannot be correlated over time. I strongly recommend doing that.

Karen J. Greenberg:

Mr. O'Harrow, because so much of this conversation stems from your earlier remarks, would you like to comment?

Robert O'Harrow (*from the audience*):

I would like to start from Jeff Jonas's remarks. The whole notion of search privacy is about to be completely altered by a new technology that I am not going to name. It will allow users to enter searches, but instead of returning what is essentially a list of results it will plot the information graphically. Let's say you start with an

e-mail address, for example. It will search across the Web for every reference to that e-mail address and bring back the results. It will then take those results and search again. So, if the e-mail address comes back with a phone

number, it will search for the phone number. If the phone number has a name, address, or company attached to it, it will instantaneously search for that, and then repeat the process again and again.

That's great for a reporter like me, but think about the implications. We have all felt comfortable sharing our e-mail address

in one place, our phone number in another, and our kids' information somewhere else because they are all separate and not linked up. In reality, we are hitting the threshold of information that is linked together: your name, your address, perhaps your financial information, and your activity online. It feels separate and, because of that, safe. In fact it is already linked together. So this protection through inefficiency is disappearing.

Jeff Jonas:

That is absolutely right. There is a lot of data in many piles. The question is, how do you amass it to get more meaning? Everyone is trying to do that in order to better compete.

The result is that by starting with an e-mail address, for example, you can find information about its owner, and then their name and address, even if that contact information isn't directly listed along with the e-mail address itself. It is a form of triangulation, although it may look like magic.

Vivian Maese:

The data is no longer only here in the United States, it is all over the world. In many cases, it



“Keep in mind that the Internet is not a free-for-all anarchic zone. Traditional common law and contract law still apply.”
Declan McCullagh

has been outsourced to different parts of the world with different conceptions of privacy and without the infrastructure for employee background checks.

One question I have been wondering about is whether the Fifth Amendment protection from self-incrimination applies to material that people type rather than speak.

Karen J. Greenberg:

Ms. Caproni, could you shed some light on the question for us?

Valerie Caproni (*from the audience*):

Remember that the Fifth Amendment protection is against compelled self-incrimination – compulsion is the issue. If you voluntarily type something in, the government is not compelling you to give that. We may compel a third party to tell us, but that is not theoretically different from your confessing to your best friend and then a grand jury asking your friend to repeat what you told him. That is not compelled self-incrimination because it is not compelling you.

Declan McCullagh:

To buttress your point, there should be no difference between what happens offline and online. Courts are good at figuring out issues at the fringes, such as determining whether a particular MySpace profile was actually updated by a specific person, for example.

Every week I read a column called “Police Blotter” about criminals and technology. There have been countless cases in which Web pages, Internet-messaging transcripts, and the like have been used as evidence in court. It is absolutely commonplace. In a case from southern California, teenage murderers were

convicted, in large part, on gruesome Internet-messaging logs.

Karen J. Greenberg:

Do you find that policymakers are generally more interested in learning how to use the tools that technology has made available or in guarding against them?

Jeff Jonas:

Often when I am asked to solve a technological problem, the very next question is how to engineer the solution in a manner that has some degree of privacy and civil liberty protections.

By talking to people in the privacy community, I get little pieces of information that allow me as a technologist to change the way I create things.

I had a conversation about data retention with David Sobel, who at the time was with the Electronic Privacy Information Center and who is now at the

Electronic Frontier Foundation. I think he is inspirational. That conversation helped me realize how I could have done some things better and how I can improve what I do in the future. As a specific example, 50 Web sites were created right after Hurricane Katrina to list the missing and the found, but sometimes the name of a missing person was listed in five different systems and the name of the same located person was listed in entirely different sites. That prevented people from finding each other. I helped create a program to bring the data from the 15 biggest Web sites together. It wound up reunifying over 100 people. But in drafting the contract for the project we required that no residual data would be left when it was over – the information would be flushed. I personally ensured that there would be nothing residual. Such an



“The policy debate comes down to who gets to peek at the data, when, and with what oversight and accountability?”
Jeff Jonas

approach would prevent re-purposing the collected data after the reunification project was concluded. I wouldn't have thought of that had I not had that conversation with David Sobel.

There aren't all that many technologists involved in the policy debate about privacy. That is important, because they are the people creating the technology being discussed.



Jeff Jonas and Karen J. Greenberg. Photo by Dan Creighton.

Robert O'Harrow (*from the audience*):

The sad truth is that Congress is operating years behind and at a much lower level of discussion than has taken place here today. It is embarrassing, almost shocking. Only a handful of lawmakers have given serious thought to this. The rest respond to problems after they happen. They make reactive policy that is, in many cases, far more costly and hurtful than helpful. It hurts the companies, it limits some of the technology's potential, and it gives us the false feeling that policy is moving forward on the issue.

Vivian Maese:

My view of the situation is not quite as dire. For much of my career, until about the turn of the century, I did not hear much conversation about technology and there were not many laws enacted to address it. People believed it to be an issue they did not have to think about. It was relegated to the back office.

In the same way that some very skilled technologists are awestruck about the pace of change, I am awestruck how Congress is gearing up for it. The laws that have been enacted so far have been on a small scale. Members of Congress need to be educated, which creates an opportunity for constructive dialogue with businesses and the public.

Declan McCullagh:

Color me a pessimist. The House Committee on Education and Labor is currently debating a bill that would require colleges and universities to implement filtering systems for peer-to-peer file-sharing services and alternatives to peer-to-peer services or else financial aid for all of their students would be cut off. That is not the sort of measured response that would suggest that Congress understands the issue.

Karen J. Greenberg:

Should the Internet should be regulated, and if so what should the priorities be?

Jeff Jonas:

The top priority should be avoiding consumer surprise. If consumers are fully informed, then they are knowingly opting in.

Karen J. Greenberg:

So there should be transparency and accountability to the people whose information is being made available. Do you think that consumers know what information is out there?

Jeff Jonas:

Not many people read Web sites' privacy statements. Nobody actually cares until it is too late.

I do not know how we are going to change that.

Declan McCullagh:

Privacy policies are written by lawyers for judges to read after a Web site has been sued. They are not written for average people. But some companies are getting better about protecting privacy. They are writing privacy statements that are more readable. Search engines are limiting their data-retention periods. In general, there are things to be optimistic about. We should not walk out of here thinking, “Oh, my God. There is all this data about me out there.” In reality, companies are governed by their reputations.

Keep in mind that the Internet is not a free-for-all anarchic zone. Traditional common law and contract law still apply. If you believe that the FBI should be allowed to intercept your telephone conversations provided that the investigators adhere to due process requirements, the same logic should apply to e-mail as well.

Public, Private, and Political Dangers

Panelists:

Prof. Todd Gitlin, Lawrence Wright

Moderator:

Prof. Stephen Holmes

Prof. Stephen Holmes:

In this panel, I would like to discuss the public and private dangers posed to privacy, and perhaps some of the cultural dimensions of the issue.

Prof. Todd Gitlin:

Privacy is always relational. It exists in relation to some force, interest, or institution that seeks to invade it. So, to speak of privacy is automatically to speak of a dialectical relationship. This point was put into place as early as December 18, 1890, in a classic article in the *Harvard Law Review* called “The Right to Privacy,” by Samuel D. Warren and Louis D. Brandeis.

The admirably compressed article sketches the necessity of a right of privacy. However, the following paragraph appears towards the end:

. . . The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel. Under this rule, the right to privacy is not invaded by any publication made in a court of justice, in legislative bodies, or the committees of those bodies; in municipal assemblies, or the committees of such assemblies, or practically by any communication in any other public body, municipal or parochial, or in any body quasi public, like the large, voluntary associations

formed for almost every purpose of benevolence, business, or other general interest; and (at least in many jurisdictions) reports of any such proceedings would in some measure be accorded a like privilege. Nor would the rule prohibit any publication made by one in the discharge of some public or private duty, whether legal or moral, or in conduct of one’s own affairs, in matters where his own interest is concerned.

This language allows for many exceptions to the general rule. Here, in the initial claim that the right of privacy is sanctioned and close to sacrosanct, there is already a recognition that privacy exists in relation to other claims, which are not only legal but moral. This takes us to the heart of the issue.

The problem is accentuated by the fact that we live in a society of surveillance. I do not mean simply police surveillance. Everywhere there are cameras, displays, self-displays, and troves of data. Everywhere one is in the business of submitting data or submitting to becoming “datafied,” if you will, in the interest of something else.

We agree that our purchases on Amazon are to be amalgamated and made available to others so they can find out that people who bought X also bought Y. We are living in the society of Facebook and MySpace. We are living in the realm of 24/7 surveillance by minicams, cell phone cameras, and the like. We are living in a society which incorporates not only the excavation of information by powerful institutions but also mutual surveillance by people volunteering data and agencies converting data to nutriment for their own institutional purposes. So the idea of what privacy entails is different today than it was in 1890, and what Warren and Brandeis were concerned with: the right to be free from



Prof. Todd Gitlin and Prof. Stephen Holmes. *Photo by Dan Creighton.*

tabloid surveillance. That concept is necessarily different than the right we understand today, or at least not automatically the same.

Someday soon, someone will write a paper equivalent to Warren and Brandeis's called "The Right to Security." I think it will present a cogent case that security is a sanctioned and legitimate right in the political, economic, and cultural circumstances that exist today.

The logic of security is impressive and also dangerous. Some of the dangers are obvious. They include abuse of information by agencies particularly, but not only, of the state. All concentrations of power can do deleterious things with information. It is not yet shrouded in the mists of history that J. Edgar Hoover, the director of the FBI, used information about President John F. Kennedy's private life in order to blackmail him. It was not so long ago that information collected by the Nixon White House was used in order to underwrite and help organize acts of burglary and assault, or that information gathered by government agencies was collected in such extravagant form so as to create the illusion that there was an agent of the FBI behind every mailbox. It is self-evident that the casting of unjust suspicion is one central danger, and related to the danger of false prosecution. Examples of post-September 11th prosecutions

are already legion.

Other dangers are less tangible. It seems to me that the fear of association is underappreciated. In a society where people are fearful, both psychologically and institutionally, playing it safe becomes a built-in feature of ordinary life. There is a risk of developing a society of universal suspicion, in which the desire to cleanse oneself of taint is always the path of least resistance and always available. The world of rampant profiling in particular is one in which a culture of suspicion becomes normal and, in fact, practical.

Practical cultures are always the ones that are the most dangerous, because they demand high-order security, expect it, and invest heavily in trying to arrange it. When the common coin of social life becomes a kind of generalized, diffuse paranoia, the world becomes uncomfortably dangerous. It is dangerous to what we purport to prize, which is autonomy in ordinary life and not only liberty to *do* but also liberty to *think*.

Given the claims of a right to security, I am certain that the right to privacy will be infringed. It is being infringed now and it will be infringed in the future. The questions are, who will infringe it and within what limits? I do not have a remedy to propose nor do I want to finesse the problem by genuflecting about something elusive called "balance." Agonizing decisions will be made, and would be made by any of us in a position in which we were ethically required to take both security and privacy seriously.

In order to avert a culture of general suspicion, a public policy of accountability needs to be brought into play. Those who exercise power will have desires, pressures, and reasons to engage in surveillance. I do not see any way around that. It is crucial that those who infringe

upon privacy be held accountable. The culture of suspicion's most dangerous feature is the termination of due process after an agency declares a question to be settled by a particular institution's reading of the security imperative. The fundamental dangers include imprisoning people without recourse to a court and excluding information from a trial that might be important in the creation of a defense.

There will be intensifying pressure for people to hide behind their fear of association, behind their fear of disclosure. I know that this will sound awfully conservative, but I believe that character-building is the only recourse against this sort of suspicion. The greatest danger in a society of suspicion is that people will surrender to their fear. There are reasons to feel fearful, and there are reasons to safeguard against that feeling, but the only protection is for people to be braver. There is no institutional substitute.

Lawrence Wright:

I have spent the last six years writing about the threat that al Qaeda poses to us. Today I am going to talk about another kind of threat, the threat that we pose to ourselves.

Karen Greenberg began the discussion today by referring to generational differences suggested by Web sites like Facebook. Younger people do not seem to resist self-disclosure in the way that older people do. But Facebook pages are self-created. Users create their own images. They may not even be telling the truth — they create their personas and have control over them. But imagine the government or creditors creating a page for you, someone else writing your Facebook page and filling in the blanks



“Those who exercise power will have desires, pressures, and reasons to engage in surveillance. I do not see any way around that. It is crucial that those who infringe upon privacy be held accountable.”

Prof. Todd Gitlin

about who you are. That is really what we are talking about here.

Why do we need to be on guard about these kinds of issues? When Senator Frank Church of Idaho led the Church Committee hearings following the abuses of Watergate, we had just emerged from an era that gave rise to FBI wiretappings of Supreme Court judges. The FBI had also wiretapped Martin Luther King, Jr., and tried to use the information they

collected to convince him to commit suicide. Such was the nature of government power then and the ill use to which it was put.

Senator Church was trying to warn against governments turning tyrannical. He was responsible for the creation of the FISA legislation. Powers granted while the government is benign can become overwhelming if turned against citizens. Any government will naturally extend its warrant and become increasingly tyrannical if left unchecked. That is why we have to be careful in granting power to them.

At the end of his administration in January 1961, President Eisenhower famously warned about the military-industrial complex. Recently, I have been working on an article for *The New Yorker* about intelligence reforms, and I have been spending a lot of time in Washington observing what one might call the “security-industrial complex.” To my mind, it is an entirely new creation whose implications have not been absorbed by most Americans.

If you look at Washington now, the city is awash in new money. Much of it has to do with the growth of the security sector. The area around Dulles Airport is ringed with high-tech security companies that are something between private industry and government. The line sepa-

rating the categories is blurred. Sixty percent of the people who work at the National Counterterrorism Center actually represent private industry. More than a third of the people who work at the CIA are private contractors. So the walls between government and private industry have come down. There are good things to say about that, but I want to alert you to the fact that something very similar to the military-industrial complex has been created.

What does this mean to the individual? We have been talking in abstract terms about the balance between privacy and security. In order to illustrate how a person whose privacy has been infringed might feel, I would like to mention two instances from my own life.

Some years ago I was in San Francisco. I went to Nordstrom and bought quite a lot of clothes. The clerk asked, "Would you like to apply for a Nordstrom credit card?"

"No," I said.

"We'll give you a 15 percent discount on all these clothes. You ought to think about it."

I totaled it up and said, "I guess I will." I applied for the credit card, she walked out of the room, came back, and said, "I'm sorry. We have turned you down." I did not want the card a moment before, but now I had been rejected.

"Why did you reject me?"

"Your credit report."

"My credit report? What's wrong with my credit report? Who gives you your credit reports?"

It was TRW, a company in both the defense and credit industries. I went home and called them. They said that if I wanted my credit report, I could file for it. So I did and they sent it to me. It was fine. It said that I had paid all my bills. I was mystified and angry that I hadn't been approved, so I called Nordstrom to find out what was going on. They told me that I hadn't been given the full report, that the one I had was different from theirs. So I called TRW again.

"Why did you give them something you didn't give me?" I asked.

It turned out to be because I hadn't given them my Social Security number, which they hadn't asked for. So I gave them the number and they sent me my real credit report. At the bottom it mentioned a lawsuit I had never heard of, a judgment against me. Had I not been an investigative reporter, it would have been very difficult to discover that the State of California had mistakenly thought I was a resident and had sued me for income tax from a movie deal I made. They could not find me, so they sued. They got a judgment and put it on my credit rating. After I found out about it, it took me a year to have it removed from the report.

The point is that everybody knew about me except me. If I had tried to buy a house during that time, I couldn't have gotten it because of a credit report I did not know about. That is one instance of a helpless individual facing the massive amount of acquired data we have been discussing.

In writing *The Looming Tower*, I spent quite a bit of time talking to jihadis and visiting the Middle East. I was certainly conspicuous. One day the FBI came to my house to ask about some telephone calls I had been making. They wanted to know who a phone number in England belonged to. I looked on my computer and found that it was a famous solicitor in London. She was defending jihadis at the time, many of whom had been sources for me.

She had called to ask me not to talk to her clients.

Next, the FBI asked me if I could identify Caroline Wright, the person who they thought was making the calls. Caroline is my daughter. She wasn't making the calls. She was away at school at the time. Moreover, how did they get her name? She is not listed on any of our phones.

"What's going on here?" I asked. "What's wrong with my talking to a lawyer in London? How did you get Caroline's name?" The investigators left at that point without answering my questions.

As a citizen, I can understand the Bureau's concern, and any other intelligence agency's concern, about who I talk to and what information I might get from them. As a reporter, I do not want them listening to my calls. As a father, I was angry because my daughter is now on a link chart connected to a solicitor who is in turn connected al Qaeda. She is two steps away from al Qaeda on the chart.

What can I do about that? I considered filing a lawsuit. I am a reporter for *The New Yorker*, and they were concerned too because much of *The Looming Tower* went into the magazine. We talked about it, and found it striking that no publication has ever sued the government for wiretapping its phones or prying into its reporters' lives. The reason for that becomes clear after some reflection. If we were to sue, the government would have discovery on any of my sources, some of whom probably told me things that the government didn't want me to know about. I didn't want to see them going to Leavenworth. I didn't want to put them in that position. From the magazine's point of view, if the discovery involved following my calls, it would also involve the follow-up calls by the factcheckers. The government would be able to

check out my sources, the factcheckers' sources, and, from that, the sources of every writer at the magazine. Suddenly everything would become transparent. A lawsuit would not be worth that.

I mention these two examples to try to convey the vulnerability that individuals face in front of such vast corporate and government power, and how incompetently that kind of power is sometimes used.

Prof. Stephen Holmes:

From the discussion today, there seem to be four factors impinging on privacy rights and the way that privacy is experienced. The first is

technological change and the digitalization of record keeping. This seems to be an ongoing, increasingly rapid process over which there is little political control. There is no way to politically choose the inventions that are created. Second, profit-seeking companies are gathering information about their customers in order to better understand them. The third factor is the government's interest in counterterrorism, which is either an actual reason for looking at information or an excuse. Finally there are the cultural norms that Karen mentioned this morning, including evolving attitudes towards privacy. The changes are to some extent generational but also have chilling effects and prevent effervescence. How is the cultural factor related to the other three, and how do all of the factors interconnect? It seems as though technology is the real driver, but that may not actually be the case.

Violations of privacy endanger not only autonomy and anonymity but also democracy. If journalists are concerned that they will not be able to maintain the confidentiality of their sources, then the citizens' right to examine their government is hindered. Bart Gellman said earlier that the president is not qualified to decide



“Everybody knew about me except me.”

Lawrence Wright

what pieces of information we should have to determine whether he's doing a good job. Geoffrey Stone powerfully said that if we become accustomed to a government spying on us, the sense that the government serves the people will be eroded.

In what other ways can invasions of privacy – either technological, commercial, or by law enforcement – harm our democratic system?

Prof. Todd Gitlin:

In determining the extent to which the problem is due to technology rather than institutional gluttony, technology is too easy to blame. The

problem with technology is not that it exists but that people have the power to use it against others. While there is no way to control technological development, it is still theoretically within the public's discretion to regulate its use.

Larry Wright's point about the security industry is quite germane. As difficult as it is to

Lawrence Wright:

I agree, in the sense that the dangers of this kind of intrusion are augmented by secrecy. The two go hand-in-hand. The more power that you have access to, the more access you have to secrets. The ordinary citizen who holds no clearance, which is how an "ordinary citizen" is now defined, has no right to information even about himself.

In thinking about your question, Prof. Holmes, I have been reflecting upon the surrender of authority, the sense that the government knows everything and is all-powerful. I have spent time talking to some very conspiracy-minded people in the Middle East. Their favorite notion is that the CIA knows everything and controls everything so that they have no power of their own. Whatever power they exercise is a fraud, they believe, because the real

power lies behind closed curtains. It is natural that they would think that. They really don't have very much power. They live in totalistic environments in which individual authority has been surrendered. We do not want to be in the same situation. However incrementally we drift down that river, that is the way the river goes. When we start to think that the government knows everything, the government starts to think that it cannot share the information it has.

I was very affected by a talk that Stephen Flynn gave here at the Center on Law and Security in April 2007. He noted that the only effective action on 9/11 was taken by a group of citizens on flight 93 who were empowered by the knowledge that they were going to die. They seized control of the plane, crashed it, and saved the lawmakers who were protecting us from knowing about these things. The Washington-area snipers were caught after a trucker heard their license plate number on his CB radio and used his truck to block their exit



Prof. Stephen Holmes and Lawrence Wright. *Photo by Dan Creighton.*

conceptualize what accountability should look like in respect to a government agency or a public entity like the armed forces, it is much harder in relation to private corporations and these strange public-private hybrids. How do you get inside them in order to hold anyone accountable? These entities are in a sense designed to confound the accountability process, and that is a very bad practice.

Listening to Larry's story about Nordstrom, it occurred to me that that if a company has a right to inspect your credit report, you should be able to see what they see and at the same time. Perhaps a lawyer can figure out how to formulate a right of simultaneous discovery. If the problem is not simply that a claim about you exists in a databank somewhere but rather that the claim is being used by a particular agency at a particular moment, then you ought to be able to participate in that moment. This concept might be too simple but I think it points in the right direction.

from a rest stop. Richard Reed, the “shoe bomber,” is the only real example we have of a person stopped during the commission of a terrorist act. A stewardess and the passengers on his flight were empowered by the knowledge that he should not be striking a match and lighting his shoe on fire.

These are the most striking instances of effective action in the war on terror, and they come from citizens, not the government. That is what could be endangered, the citizens’ feeling that the country belongs to them and is their responsibility rather than the government’s.

Prof. Todd Gitlin:

One of the most chilling moments in Franz Kafka’s *The Trial* occurs when Josef K. is informed that there is a rule being applied to his case but he is not qualified to see it. That is the moment that must be prevented by accountability.

Prof. Stephen Holmes:

Government secrecy may be one reason why we distrust the claim that reducing privacy leads to more security. It seems that when citizen privacy is reduced, government secrecy is increased. Security is then adversely affected, because governments that act in secret do not share information with people who could use it.

Prof. Gitlin mentioned the challenges to accountability posed by hybrid entities, those that are between public and private. It turns out that accountability can be avoided by hiding the ball. Within the government, programs can continue even after having been banned by Congress if they are shifted elsewhere. That destroys the democratic accountability process.

Government has its own rules about what it must display and expose. Industry has its rules about what it can conceal and expose. In combination they increase the ability to avoid oversight, which can remove the incentives to take reasonable care.

EXCERPTS FROM THE QUESTION AND ANSWER SESSION

Question (from the audience):

Prof. Gitlin, could tell us a bit more about your notion of character? Are there any historical examples of a certain character type that helped to preserve democracy or developed in a way that we could encourage?

Prof. Todd Gitlin:

McCarthyism was, in part, a direct, government-instigated assault on people’s rights. It led to people losing their jobs, among other consequences, and had an enormous spillover effect on society. Senator McCarthy was finished as a political force by 1954, but as late as 1960 I met fellow students who were afraid to sign petitions. That fear had been instilled in them.

Something happened over the following few years so that people stopped caring what the authorities thought of them. They started mocking the authorities. They became indifferent to whether their names appeared on lists. Any attempt at a sociological explanation for this quickly becomes circular – people cease to be afraid because they cease to be afraid. It happens in some societies, and I do not know how to account for it.

Lawrence Wright:

After 9/11, many of us felt as though we would now have to stand for something, that it was our turn. We had gotten off easily as a generation. We did not fight the Civil War; we did not live through the Depression or World War II. It was our turn to step up to the plate, and many of us did. I have spoken many soldiers and Marines in the last several years, and their degree of moral seriousness is inspiring.

But that notion was essentially put to sleep in the population at large. We were told that we did not need to be serious, that the government would take care of us. We were told to go shopping, to do what we had been doing. That was a

tragedy in our country. It was a moment when we could have been rallied and we failed. We let the government take control, and look where we are now. On 9/12, the whole world was bending in our direction. How will we ever get back to that point?

Prof. Stephen Holmes:

In the previous panel discussion, Robert O’Harrow gave a hair-raising description of a technology that will allow all of the information about us that is currently segmented into non-communicating parcels to be put together. That idea has led me to consider how we conceive of personal identity, and it is related to character in some way.

Personal identity is intertwined with our capacity to dose out information about ourselves. We can dose layers of interiority to people according to whether they are intimate friends or relative strangers. The separation allows us to

keep our sense of who we are as autonomous beings. We can say something in one context that doesn’t immediately bleed into another.

If it is true that this technological revolution is unstoppable and accelerating to the point where every conversation can be listened to, then it is going to have a tremendous impact on how we operate as human beings. It will affect not only our relationship with the government but also our social existence and our sense of personhood.

Prof. Todd Gitlin:

One possible response is that some people may decide to throw off the traditional boundary between the private and the public. As the powers of the state enlarged themselves during the Cold War, a group of cultural figures, particularly writers, emerged. They said that they’d

protect themselves by stripping naked. Allen Ginsberg, who was quite sophisticated in his understanding of the world of surveillance, made that decision early on. He basically said, “In a society like this, I will have no secrets.” The way to belittle the strategy is to call it exhibitionism, but I wouldn’t reduce it to that.

I spent some time in Hungary in 1988, a year before the overturn of the Communist regime. I met a dissident who had essentially adopted this strategy, although very few others had the nerve to do it. He lived his entire life with the understanding that he was always

under surveillance. He simply decided not to care. Some people have to be willing to say that there is less, or nothing, to fear if they take the stoic route and remove the harm.

As I understand stoic philosophy, the trick is recognizing that the world is full of dangers but only things within your control can get to you. You can

control your interpretation of the dangers you face, and deciding not to be afraid eliminates fearsomeness. Some people, I think, will have to decide to live in that fashion.

Prof. Stephen Holmes:

You cannot just be stoic for yourself if other people will get in trouble as a consequence.

Prof. Todd Gitlin:

No, that is why accountability is crucial. These things have to be contested. In the end, what is required is a refusal of innocence. We suffer from what one writer, after 9/11, called “serial innocence.” Innocence is always ending in America. We were innocent until November 22, 1963; we were innocent until 9/11. It is an absurdity.

In the ’60s, when I was a student activist, I was hardly ever involved in anything especially



“When we start to think that the government knows everything, the government thinks that it cannot share the information it has.”

Lawrence Wright

dangerous or subversive. From an early age, however, I was mindful of the likelihood that some government agency would be interested in what I was saying, certainly on the telephone. I simply decided to live with that. Joking about it helped.

The power of surveillance mechanisms to freeze you is within your control. Mississippi was a terror state before the civil rights activists went down there to overthrow it. It was a terror state while they were there. It was just as fearsome one time as the other. Some people had to simply decide that it wasn't going to stop them. I know that sounds pious, but that is, in fact, how institutions are pushed back.

Prof. Stephen Holmes:

I believe that there was a rule in Communist-era Poland and Hungary never to tell the police an irrelevant fact, because they would use it later against someone you know. The question isn't whether or not you have enough courage to ignore the fact that you are being surveilled. Innocently giving information that could be used by the authorities against someone else is a problem. That will chill your communication no matter how stoic you are. It is not a matter of your own character.

Prof. Todd Gitlin:

Yes, that is true. That is some of the innocence that will be given up. In a setting like that, everybody understands there are conversations you don't have indoors.

Lawrence Wright:

Where are we going with all of this, and what kind of people are we going to become? We are at a kind of turning point. Our becoming like the Hungarians or the Czechs, under a thumb, constantly guarding our own conversations, is not inevitable. We have to be especially on guard about secrecy.

I would be the last person to dismiss the threat of terrorism because I have studied it

closely enough to recognize how profound a danger it is. But when Osama bin Laden attacked America, he was posing two questions: What is Islam, and what is America?

Islam is in the middle of a turbulent discussion about where it is going and what it should be. We have a great interest in that discussion but no real ability to control it.

In defining America, we are all responsible for the answer. We have made a considerable number of changes in our country without having addressed them. Last year I went to Philadelphia and visited the Liberty Bell. I was struck by the fact that I had to take off my belt and my shoes and empty my pockets. You have to take off your shoes to visit the Liberty Bell? You can't go up into the Statue of Liberty anymore. These are just symbols, but they are deeply resonant symbols of things we have given up without even thinking about them, without even asking ourselves if the sacrifice is worth it. To me, they represent compromises of the kind of people we are.

Prof. Gitlin talked about being braver. I think that is a good point in some ways. We do live with risk, we just do not want to acknowledge it. We compromise on our civil liberties, and other things that are dear to us, with the idea that we are going to become safer. Yet there is not much evidence that we are safer, because we never truly know when we are safe. If we pretend that we are now safe on airplanes, we may not be safe on the subways or in our apartment buildings. We are always going to be at risk. We are missing a healthy acknowledgment of that, and an appreciation of the fact that these liberties were hard fought for. They are rare in human history. Once surrendered, they are very hard to regain.

When people ask me about al Qaeda, I always say, "Al Qaeda is not going to win. It stands against human history. It has nothing to offer to any of the people that follow it." But I think that unless we remember the lessons of our own history, we won't win either.

INDEX

A

Access to records, 90–91, 92
Accountability, 92, 97, 111–112, 116
ACLU. *See* American Civil Liberties Union (ACLU)
Administrative subpoenas, 97
Adversarial process, secrecy and, 30, 32, 34, 40, 56
AIPAC, 27, 45
Algeria, Islamic extremism in, 65
Al-Haramain Islamic Foundation, 46
Almindhar, Khalid, 95
al Qaeda, 112, 114, 118
Alshehri, Wail, 95
Amazon, 110
American Civil Liberties Union (ACLU), 36, 46, 49, 61, 67, 102
The American Experience, 30
American Newspaper Association, 22
America OnLine, 106
Anonymity, 103, 106, 115
Apple Computers, 104
Army-McCarthy Hearings, 65–66
Ashcroft, John, 51, 57, 76
Assets, secrets as, 32
Atkinson, Rick, 39
Atta, Mohammed, 95
Attorney-client privilege, 50
Attorney General Guidelines, 75–76, 94
Attorneys, willingness to represent defendants, 67
Autonomy, 77, 80, 84, 86, 115

B

Banks, privacy and, 101
Bank Secrecy Act, 93
Bay of Pigs, 32–33
Beeson, Ann, 36
Bharatiya Janata Party, 33
Billy, Joseph, 94
bin Laden, Osama, 29, 118
Biological weapons, 79

“Black sites,” 60
Bradlee, Ben, 26
Brandeis, Louis D., 110–111
British Foreign Service, 27
Brosnahan, Jim, 51
Brown, Harold, 26
Bureaucracy, secrecy and, 31–32
Bureau of Prisons, 50
Bush, George W., 23, 26, 36, 39, 41, 66, 74, 88, 92

C

California, Holocaust cases in, 81
Cambodia, incursion in, 25
Carnivore DCS1000, 105
Carter, Jimmy, 26, 40, 88
Castro, Fidel, 32–33
Cellular telephones, 102
Central Intelligence Agency (CIA)
 “black sites,” 60
 censorship by, 54
 changes within, 65
 conspiracy theories and, 115
 information security technology and, 102
 kidnapping by, 16, 45
 private contractors and, 113
 secret prisons, 15–17, 28
 surveillance by, 82
 war on terror and, 64–65
Character and democracy, 116–117
Chemical weapons, 79
Cheney, Dick, 16, 21, 31
Child Online Protection Act, 106
“Chilling effect,” 91
ChoicePoint, 82–83
Chou En-lai, 22
Church, Frank, 112
Church Committee, 75–76, 112
CIA. *See* Central Intelligence Agency (CIA)
Civil liberties oversight board, 97
Civil liberties violations, 66
Civil rights movement, 118

Classified Information Procedures Act (CIPA), 48, 60
Clinton, Bill, 15, 89, 98
Cognition, secrecy and, 31–32
COINTELPRO, 75
Cold War, 58, 117
Combat Status Review Tribunal, 22
Communists, 67
Computer & Internet Protocol Address Verifier (CIPAV), 105
Confidentiality of sources, 31, 96, 115
Congress
 authorization of intelligence, 23
 FBI, oversight of, 76–77
 Justice Department, oversight of, 41
 oversight of intelligence, 41–43, 59
 regulation of intelligence, 88–89
 technology and, 108
Conspiracy theories, 115
Constitutional Convention, 65
Consumer protection, 108–109
Corporations, privacy and, 81, 115
Counterintelligence Corps, 25
Counterterrorism, 115
Credit fraud, 103
Credit reports, 113, 115
Creel, George, 14
Criminal justice system, secrecy and, 47
Cromwell, Oliver, 20
Cultural concepts of privacy, 100–101, 115
Czechoslovakia, surveillance in, 118

D

Datamining, 95, 102
Data revolution, privacy and, 77–81, 90
Davis, Dennis, 40
D-Day, 22, 31
Defense attorneys, 46–47
Defense Department, 33
Delayed notice warrants, 99
Democracy, secrecy and, 30, 63
Department of Defense, 33
Department of Health and Human Services, 98
Department of Homeland Security, 24–25
Department of Justice. *See* Justice Department

DeRosa, Mary, 95
Digitalization of records, 115
Disclosure, 59
Disinformation, 32
Divided government, 43
Doumar, Robert, 52, 56
Downie, Len, 28
Dratel, Joshua, 52, 63
Drug Enforcement Agency, 98–99
Due process, FISA and, 48
Dunham, Frank, 51–52

E

Easterbrook, Frank, 44
Eisenhower, Dwight D., 22, 30, 66, 112
Electronic Communications Privacy Act, 93
Electronic Frontier Foundation, 107
Electronic information, retention of, 101–103
Electronic Privacy Information Center, 107
Electronic surveillance, 80, 88
Ellsberg, Daniel, 66
E-mail
 privacy and, 106
 retention of, 101–102
 surveillance of, 90
Encryption, 104–105
Enemy combatants, 41, 52
England, secrecy in, 20
Ennis, Bruce, 55
Espionage Act, 27, 45
Executive privilege, 66
Exigent letters, 62

F

Facebook, 74, 100, 105, 110, 112
Fair Credit Reporting Act, 93
FBI. *See* Federal Bureau of Investigation (FBI)
Federal Bureau of Investigation (FBI)
 access to records, 90
 attorneys, investigation of, 50–51
 Congressional oversight, 76–77
 data revolution and, 78
 electronic surveillance by, 105
 judicial oversight, 76

national security letters, 17, 23, 61–63, 82, 85, 93–94
Office of General Counsel, 75
privacy and, 74–76
“sneak and peek” searches, 90, 99
surveillance by, 82–83, 113
trust of, 83
wiretapping by, 112
Federal Defenders Office, 52
Feingold, Russell, 41
Fifth Amendment, 107
First Amendment, 61, 66, 76, 86, 91–92, 96
FISA. *See* Foreign Intelligence Surveillance Act (FISA)
Flight 93, 115
Flynn, Stephen, 115
Ford, Gerald, 88
Foreign Intelligence Surveillance Act (FISA)
 accountability and, 97
 amendments to, 76
 balancing of interests under, 89
 creation of, 112
 data revolution and, 77–78
 notice, absence of, 97, 99
 oversight under, 91–92, 97
 prerequisites for surveillance under, 91
 privacy and, 88–99
 reforms, 89
 roving wiretaps, 98
 secrecy and, 96
 “sneak and peek” searches, 98–99
 warrants under, 48
Foreign Intelligence Surveillance Court, 17, 45, 48
Fourth Amendment, 80, 84, 86, 91–92, 96
Frankfurter, Felix, 44
Franklin, Benjamin, 75
Freeborn John, 20–21
Freedom of Information Act, 29, 60–61
Fulbright, William J., 25, 42

G

Gag orders, 62
Gates, Robert, 41
Gellman, Barton, 62

Generational concepts of privacy, 74, 100
Genuine secrets, 47–48, 56
Germany
 bureaucracy in, 31
 CIA kidnapping in, 16, 45
 Holocaust cases in, 81
Gideon, Clarence, 52
Gideon's Trumpet, 52
Ginsberg, Allen, 117
Gladwell, Malcolm, 33
Gleeson, John, 54
Globalization, 101
Global Positioning System (GPS), 102
Google, 105
Grand juries, 85, 91, 98
Guantánamo Bay, 22, 45, 55, 57, 67
Gulf War, 39

H

Habeas corpus, 20
Hackers, 103
Hamdi, Yaser, 45, 50–52, 54, 56
Harlan, John F., 53
Harvard Law Review, 110
Haynsworth, Clement, 54
Health and Human Services Department, 98
Helms, Richard, 54
Hicks, David, 22, 50, 52
Hindi, Abu Issa al-, 24
Hitler, Adolf, 23
Holocaust, 23, 80–81
Homeland Security Department, 24–25
Hoover, J. Edgar, 111
House Committee on Education and Labor, 108
Hungary, surveillance in, 117–118
Hurricane Katrina, 107
Hussein, Saddam, 66

I

IBM, 102
Identity theft, 103
Incoherence, secrecy and, 33
Incompetence, secrecy and, 31, 64
Indefinite detention, 55

India, nuclear weapons and, 33
Information revolution, privacy and, 77–81,
90–91
Information security technology, 102–103
In-Q-Tel, 102
Inspector General, 36–37, 62, 77, 93
Insurance companies, privacy and, 81
Intelligence warrants, 48
Interagency secrecy, 34–35, 41
Internet, privacy and, 108–109
Internet service providers (ISPs), 105
Iraq
 secrecy and, 17
 weapons of mass destruction in, 66
Iraq War, 66
Islam, 118
Islamic extremism, 64–65
“Islamofascism,” 64

J

Jaffer, Jameel, 36, 52
Japanese-Americans, concentration camps
 for, 67
Japanese in concentration camps, 55
Joint Committee on Atomic Energy, 42
Judicial oversight, 76
Judiciary, secrecy and, 41
Justice Department
 attorneys, conditions on, 50–52
 Congressional oversight, 41
 fear and anger in, 64
 guidelines, 76
 Inspector General, 36–37, 62, 77, 93
 national security letters and, 17, 37, 62
 privacy and, 106

K

Kafka, Franz, 116
Keith, Damon, 52
Kennan, George F., 33
Kennedy, John F., 22, 38, 111
Kerr, Donald, 93
Khalifa, Jamal, 29
King, Garr M., 46

King, Martin Luther, Jr., 112
Kissinger, Henry, 22–23

L

Laos, bombing of, 25
Leahy, Patrick, 41
Leaks, 24, 28–29
Lee, Wen Ho, 26–27
Lewis, Anthony, 52
LexisNexis, 83
Libby, Scooter, 16
Liberty Bell, 118
Libya, arms sales to, 56
Lilburne, John, 20–21
Lindh, John Walker, 51
Link analysis, 95
LinkedIn, 105
Liptak, Adam, 47
London Times, 28
Long Parliament, 20
The Looming Tower, 113–114

M

Madison, James, 65
Madrid bombings, 91
Mao Zedong, 22
Marchetti, Victor, 54
Masri, Khaled el-, 16, 45
Matalin, Mary, 16
Mayfield, Brandon, 91
McCarthy, Joseph, 66–67, 116
McCarthyism, 66, 116
“Metalaws,” 104
“Military-industrial complex,” 112–113
Mississippi, civil rights movement in, 118
Mosaic theory, 45, 62
Moussaoui, Zacarias, 52
Moynihan, Daniel Patrick, 30–34, 38
MySpace, 100, 105, 107, 110

N

Nashiri, Abd al-Rahim al-, 22, 54
National Counterterrorism Center, 113

National security, secrecy and, 58–65
National Security Agency (NSA) wiretapping program, 17, 23, 45–46, 49, 59, 76–78
National security letters, 17, 23, 36–37, 61–64, 82, 85, 93–94, 98
Neutron warhead, 26
Newman, Donna, 51
The New Yorker, 112
New York Police Department, Republican
National Convention and, 23–24
New York Times, 24, 28–29, 31, 47, 53, 63, 66, 78, 96
9/11
 access to records after, 91–92
 Attorney General Guidelines after, 94
 deference to executive after, 41
 electronic surveillance after, 88
 FBI, impact on, 75
 FISA warrants after, 48
 Flight 93, 115
 FOIA, impact on, 62
 interagency information sharing after, 36
 “metalaws” and, 104
 “paralaws” and, 104
 popular response to, 116–118
 privacy after, 37
 secrecy after, 15, 44, 58
 significance of, 66
 technology, effect on use of, 102
9/11 Commission, 97
Nixon, Richard, 22, 31, 42, 53, 66, 88, 111
Nordstrom, 113
North Korea, nuclear weapons and, 26
NSA wiretapping program. *See* National Security Agency (NSA) wiretapping program
NSLs. *See* National security letters
Nuclear weapons
 Cold War, during, 58
 India and, 33
 North Korea and, 26
 The Progressive and, 53–55
 terrorists and, 79
 U.S. policy regarding, 42

O

O’Connor, Sandra Day, 52, 89
Office of General Counsel (FBI), 75
Office of Legal Counsel, 17, 35, 50, 63, 89
O’Harrow, Robert, 82
OSX operating system, 104

P

Packard, David, 42
Padilla, Jose, 22, 45, 50–51, 55
Pakistan, Islamic extremism in, 65
“Paralaws,” 104
Partisanship, secrecy and, 33–34
Patel, Andrew, 51
Patriot Act
 access to records under, 91
 national security letters under, 36–37, 61–62, 82, 93
 oversight under, 91
 prerequisites for surveillance under, 91
 privacy and, 74–75, 88–99
 reauthorization, 82
 roving wiretaps, 98
 “sneak and peek” searches, 98–99
Peer-to-peer file sharing, 108
Pelosi, Nancy, 18
Pentagon Papers, 31, 53, 55, 66
Personal identity, 117
Pike Committee, 75–76
Pincus, Walter, 16, 65
Plenary intelligence authority, 89
Poland, surveillance in, 118
Political secrets, 48–49
Powell, Colin, 25
Press, role of, 95–96
Priest, Dana, 59, 65
Privacy
 banks and, 101
 corporations and, 81, 115
 cultural concepts of, 100–101, 115
 dangers to, 110–118
 data revolution and, 77–81, 90–91
 e-mail and, 106
 FBI and, 74–76
 FISA and, 88–99

- generational concepts of, 74, 100
- global information network and, 100–109
- historical perspective, 74–86
- information revolution and, 77–81, 90–91
- insurance companies and, 81
- Internet and, 108–109
- Justice Department and, 106
- 9/11, after, 37
- Patriot Act and, 74–75, 88–99
- private sector and, 83–84, 86, 91, 115
- self-government and, 81
- suspicion and, 111–112
- technology and, 104, 115
- telecommunications and, 88–99
- terrorism and, 79
- Privacy Act, 75, 89–90
- Private sector, privacy and, 83–84, 86, 91, 115
- Privileged communications, 110
- The Progressive*, 53–55
- Prosecutors, 46–47
- Psychology, secrecy and, 32–33

R

- Radack, Jesselyn, 50–52, 56–57
- Reagan, Ronald, 88
- Reed, Richard, 116
- Regulation, secrecy as, 38
- Rendition, 15, 67
- Republican National Convention, 23–24
- Retention of records, 101–103
- Ridge, Tom, 24–25
- Risen, James, 59, 65
- Roosevelt, Franklin, 14
- Roundheads, 21
- Roving wiretaps, 98
- Rule of law, 92
- Rumsfeld, Donald, 33–34, 41

S

- SAMs (Special Administrative Measures), 50, 57
- Saudi Arabia, Islamic extremism in, 65
- Scarfo, Nicodemo, 105
- Schwarzkopf, Norman, 39

- Search and seizure, 80
- Search engines, 106
- Secrecy
 - bureaucracy and, 31–32
 - cognition and, 31–32
 - criminal justice system and, 47
 - decisionmaking and, 30–43
 - democracy and, 63
 - England, in, 20
 - FISA and, 96
 - historical perspective, 18–29
 - incoherence and, 33
 - incompetence and, 31, 64
 - interagency secrecy, 34–35, 41
 - Iraq and, 17
 - judiciary and, 41
 - national security and, 58–65
 - 9/11, after, 15, 44, 58
 - partisanship and, 33–34
 - psychology and, 32–33
 - regulation, as, 38
 - South Africa, in, 40
 - Soviet Union, in, 20
 - terrorism and, 58–59
 - torture and, 22, 27, 54–55
 - War on Terror and, 44–56
- Secret trials, 66–67
- Security, right to, 111–112
- “Security-industrial complex,” 113
- Self-government, privacy and, 81
- Self-incrimination, 107
- Senate Foreign Relations Committee, 25, 42
- September 11. *See* 9/11
- “Serial innocence,” 118
- Simmel, Georg, 32
- Sixth Amendment, 50, 52
- “Sneak and peek” searches, 90, 98–99
- Sobel, David, 108
- South Africa, secrecy in, 40
- Soviet Union, secrecy in, 20
- Special Administrative Measures (SAMs), 50, 57
- Special Forces, 15
- Special Operations Command, 15, 19
- Split government, 24
- Spyware, 105

Stalin, Joseph, 23
Star Chamber, 20
State secrets privilege, 45
Statue of Liberty, 119
Stewart, Lynne, 50, 56–57
Stimson, Charles, 57
Stoicism, 118
Subpoenas, 61, 85, 91, 98, 105
Suqami, Satam M. A. al, 95
Surveillance
 electronic surveillance, 80, 88
 wiretapping (*See* Wiretapping)
Suspicion, privacy and, 111–112
Swire, Peter, 103
Switzerland, Holocaust cases in, 80–81
Syria, Islamic extremism in, 65
Systems Research and Development, 102

T

Tactical secrets, 48–49
Technology, privacy and, 104, 115
Telecommunications, privacy and, 88–99
Telephones, surveillance of, 90
Terrorism
 privacy and, 79
 secrecy and, 58–59
Terrorist Surveillance Program (NSA), 17, 23, 45–46, 49, 59, 76–78
Torture
 authorization of, 63
 civil liberties and, 67
 secrecy and, 22, 27, 54–55
Total Information Awareness Program, 95
Totalist argument, 44–46
The Trial, 116
Truman, Harry, 33
TRW, 113

U

Unified government, 40
USA Patriot Act. *See* Patriot Act

V

Venona decryptions, 33
Vietnam War, 53

W

Walter Reed Army Hospital, 15–16
War on Terror
 CIA and, 64–65
 open-ended nature of, 66–67
 secrecy and, 44–56
Warrants
 delayed notice warrants, 99
 FISA warrants, 48
 intelligence warrants, 48
Warren, Robert, 55
Warren, Samuel D., 110–111
Washington Post, 16, 26, 28–29, 36–39, 45, 53, 62–63, 66, 82–84, 94, 96
Watergate, 66, 88, 112
Weber, Max, 31, 43
Westlaw, 83
Wilson, Charles, 66
Wilson, Edwin, 56
Wilson, Joe, 16
Wilson, Woodrow, 14
Windows, 104
Wiretapping
 FBI, by, 112
 lawfulness of, 66
 NSA program, 17, 23, 45–46, 49, 59, 76–78
 ordinary criminal proceedings, 48–49
 roving wiretaps, 98
The Wizard of Oz, 65
World Trade Center bombing (1993), 50

Y

Yoo, John, 44, 54

ABOUT THE CENTER

Founded in 2003, The Center on Law and Security is an independent, non-partisan, global center of expertise designed to promote an informed understanding of the major legal and security issues that define the post-9/11 environment. Towards that end, the Center brings together and to public attention a broad range of policymakers, practitioners, scholars, journalists and other experts to address major issues and gaps in policy discourse and to provide concrete policy recommendations.

Executive Director

Karen J. Greenberg

Faculty Co-Directors

Noah Feldman
David M. Golove
Stephen Holmes
Richard Pildes
Samuel Rascoff

Board of Advisors

Daniel Benjamin
Peter Bergen
Rachel Bronson
Roger Cressey
Viet Dinh
Joshua Dratel
Farhad Kazemi
Richard Greenberg
Martin Gross
Bernard Haykel
Scott Horton
Judge Kenneth Karas
Priscilla Kauff
Dana Priest
Andrew Peterson,
Alumni Advisor

Fellows, Past and Present

Peter Bergen
Sidney Blumenthal
Peter Clarke
Paul Cruickshank
Amos Elon
Judge Baltasar Garzón
Barton Gellman
Tara McKelvey
Dana Priest
Nir Rosen
Barry Sabin
Michael Sheehan
Craig Unger
Michael Vatis
Robert Windrem
Lawrence Wright

Staff

Nicole Bruno
Director of Programs
Daniel Freifeld
*Director of International
Programs*
Jeff Grossman
Editor
Francesca Laguardia
Director of Research
Maggie McQuade
Executive Assistant
David Tucker
*Director of Development
and Business Affairs*

www.lawandsecurity.org



THE CENTER ON LAW AND SECURITY
AT THE NEW YORK UNIVERSITY SCHOOL OF LAW

110 West Third Street, Suite 217

New York, NY 10012

(212) 992-8854

CLS@exchange.law.nyu.edu