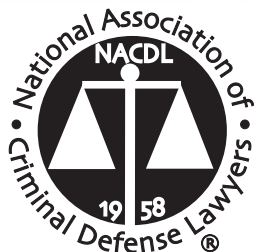




The Fourth Amendment in the Digital Age NACDL Symposium

Andrew Guthrie Ferguson
Professor of Law
UDC David A. Clarke School of Law

REPORTER





Supported by a grant from the Foundation for Criminal Justice.

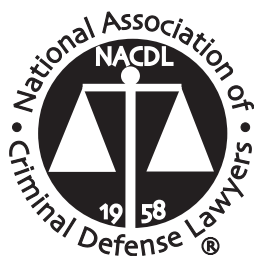
Copyright © 2016 National Association of Criminal Defense Lawyers



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>. It may be reproduced, provided that no charge is imposed, and the National Association of Criminal Defense Lawyers is acknowledged as the original publisher and the copyright holder. For any other form of reproduction, please contact NACDL for permission.

Cover Images:

© VoodooDot | shutterstock — surveillance
© Alex Stokes | Dollarphotoclub — hand



For more information contact:

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

1660 L Street NW, 12th Floor

Washington, DC 20036

Phone: 202-872-8600

www.nacdl.org

This publication is available online at

www.nacdl.org/FourthAmendmentInTheDigitalAge

The Fourth Amendment in the Digital Age

NACDL Symposium

E.G. "Gerry" Morris

President, NACDL
Austin, TX

Gerald B. Lefcourt

President, FCJ
New York, NY

Theodore Simon

Immediate Past-President, NACDL
Philadelphia, PA

Norman L. Reimer

Executive Director, NACDL
Washington, DC

Kyle O'Dowd

Associate Executive Director
for Policy, NACDL
Washington, DC

Jumana Musa

Sr. Privacy and National
Security Counsel, NACDL
Washington, DC

Andrew Guthrie Ferguson

Professor of Law
UDC David A. Clarke
School of Law
Reporter
Washington, DC



Table of Contents

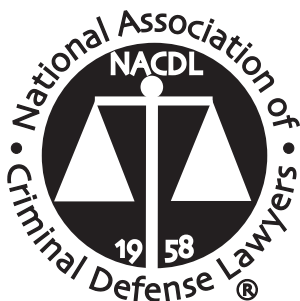
About the National Association of Criminal Defense Lawyers (NACDL)	3
About the Foundation for Criminal Justice (FCJ)	4
Acknowledgments.	5
Foreword.	6
Executive Summary.	7
Symposium Overview	12
<p>Dean Claudio Grossman, <i>Dean of American University Washington College of Law and the Raymond I. Geraldson Scholar for International and Humanitarian Law</i></p> <p>Theodore Simon, <i>President, National Association of Criminal Defense Lawyers</i></p>	
1. New Developments in Surveillance Technology: How the Government Collects, Searches, Stores, and Shares Information	14
<p>MODERATOR:</p> <p>Jennifer Daskal, <i>Assistant Professor of Law, American University Washington College of Law</i></p> <p>DISCUSSANTS:</p> <p>Catherine Crump, <i>Assistant Clinical Professor of Law; Associate Director, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law</i></p> <p>Elizabeth Goitein, <i>Co-Director of the National Security Project, Brennan Center for Justice at NYU School of Law</i></p> <p>Joseph Lorenzo Hall, <i>Chief Technologist, Center for Democracy & Technology</i></p> <p>Eric Wenger, <i>Director of Cybersecurity and Privacy Policy for Global Government Affairs, Cisco Systems</i></p>	
2. Challenges to the System: Prosecutors, Judges, and Defense Attorneys in the Digital Age	22
<p>MODERATOR:</p> <p>E.G. "Gerry" Morris, <i>President-Elect, National Association of Criminal Defense Lawyers</i></p> <p>DISCUSSANTS:</p> <p>Hanni Fakhoury, <i>Senior Staff Attorney, Electronic Frontier Foundation</i></p> <p>Neema Singh Guliani, <i>Legislative Counsel, American Civil Liberties Union</i></p> <p>Jim Harper, <i>Senior Fellow, CATO Institute</i></p> <p>Orin Kerr, <i>Fred C. Stevenson Research Professor of Law, George Washington University Law School</i></p>	
3. A Conversation with Joseph P. Nacchio	29
<p>Joseph P. Nacchio, <i>Former Chairman and CEO, Qwest Communications International</i></p> <p>Norman L. Reimer, <i>Executive Director, National Association of Criminal Defense Lawyers</i></p>	
4. Law and Policy: A Path Forward for the Constitution, Courts, Congress, and Law Enforcement ...	30
<p>MODERATOR:</p> <p>Jeff Rosen, <i>President and CEO, National Constitution Center; Professor of Law, George Washington University Law School</i></p> <p>DISCUSSANTS:</p> <p>Ahmed Ghappour, <i>Visiting Professor, UC Hastings College of the Law; Director, Liberty, Security and Technology Clinic</i></p> <p>David Lieber, <i>Senior Privacy Policy Counsel, Google</i></p> <p>Greg Nojeim, <i>Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy and Technology</i></p> <p>Kenneth Wainstein, <i>Partner, Cadwalader, Wickersham & Taft LLP; Former Homeland Security Advisor; Former Assistant Attorney General for National Security, DOJ; Former United States Attorney for the District of Columbia</i></p>	
Summary and Recommendations	40
Endnotes	43
Appendix A: Biographies	46
Appendix B: Symposium Agenda	53

About The National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) is the preeminent organization in the United States advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with a crime or wrongdoing. NACDL's core mission is to: *Ensure justice and due process for persons accused of crime ... Foster the integrity, independence and expertise of the criminal defense profession ... Promote the proper and fair administration of criminal justice.*

Founded in 1958, NACDL has a rich history of promoting education and reform through steadfast support of America's criminal defense bar, *amicus curiae* advocacy and myriad projects designed to safeguard due process rights and promote a rational and humane criminal justice system. NACDL's approximately 9,000 direct members — and 90 state, local and international affiliate organizations totalling up to 40,000 members — include private criminal defense lawyers, public defenders, active U.S. military defense counsel, and law professors committed to preserving fairness in America's criminal justice system. Representing thousands of criminal defense attorneys who know firsthand the inadequacies of the current system, NACDL is recognized domestically and internationally for its expertise on criminal justice policies and best practices.

The research and publication of this report was made possible through the support of individual donors and foundations to the Foundation for Criminal Justice, NACDL's supporting organization.



For more information contact:

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

1660 L Street NW, 12th Floor

Washington, DC 20036

Phone: 202-872-8600

www.nacdl.org

This publication is available online at

www.nacdl.org/FourthAmendmentInTheDigitalAge



About The Foundation for Criminal Justice (FCJ)

The Foundation for Criminal Justice (FCJ) is organized to preserve and promote the core values of America's criminal justice system guaranteed by the Constitution — among them due process, freedom from unreasonable search and seizure, fair sentencing, and access to effective counsel. The FCJ pursues this goal by seeking grants and supporting programs to educate the public and the legal profession on the role of these rights and values in a free society and assist in their preservation throughout the United States and abroad.

The FCJ is incorporated in the District of Columbia as a non-profit, 501(c)(3) corporation. All contributions to the FCJ are tax-deductible. The affairs of the FCJ are managed by a Board of Trustees that possesses and exercises all powers granted to the Foundation under the DC Non-Profit Foundation Act, the FCJ's Articles of Incorporation, and its Bylaws.



For more information contact:

FOUNDATION FOR CRIMINAL JUSTICE

1660 L Street NW, 12th Floor

Washington, DC 20036

Phone: 202-872-8600

www.nacdl.org/foundation

This publication is available online at

www.nacdl.org/FourthAmendmentInTheDigitalAge

Acknowledgments

NACDL would like to thank the Foundation for Criminal Justice, the American University Washington College of Law (WCL) and the *Criminal Law Practitioner* for their support of this symposium and Professor Andrew Guthrie Ferguson¹ for drafting this report. We would also like to thank the following NACDL staff for their careful editing and helpful suggestions: Jumana Musa, Sr. Privacy and National Security Counsel; Norman L. Reimer, Executive Director; Kyle O'Dowd, Associate Executive Director for Policy; Quintin Chatman, Editor of *The Champion*; Ivan J. Dominguez, Director of Public Affairs & Communications; Lisa Schrade, National Affairs Assistant; and Cathy Zlomek, NACDL Art Director, for the design of the report.

This report would not have been possible without the insightful contributions of our esteemed symposium conference panelists, identified throughout the report and in Appendix A. Sincerest gratitude goes to the following individuals, who worked behind the scenes to make the symposium possible: at WCL, Dean Claudio M. Grossman; Tanisha Santos, Assistant Director of the Office of Special Events and Continuing Legal Education; Raleigh Mark, Editor-in-Chief of the *Criminal Law Practitioner*; Robert Northdurft, Executive Editor, *Criminal Law Practitioner*; and Trevor Addie, Blog Editor, *Criminal Law Practitioner*. At NACDL, Jumana Musa, Sr. Privacy and National Security Counsel; Norman L. Reimer, Executive Director; Kyle O'Dowd, Associate Executive Director for Policy; Ivan J. Dominguez, Director of Public Affairs & Communications; Angelyn Frazer-Giles, Director of State Legislative Affairs and Special Projects; Cathy Zlomek, NACDL Art Director; Jennifer Renae Waters, Graphic Designer; and former NACDL staff Mason Clutter, former National Security and Privacy Counsel; Elsa Ohman, former National Affairs Assistant; Isaac Kramer, former Public Affairs and Communications Assistant and Jason Rogers, Freelance Graphic Designer. A special thank you to E.G. "Gerry" Morris, President, National Association of Criminal Defense Lawyers, for his vision, support and contributions to the symposium.



Foreword

The digital age has made possible modes of communication never imagined just a few decades ago. Email, text messaging, and social media are now integral parts of our personal and professional lives. These ubiquitous new means of communication come at a price: they afford opportunities for governments not only to intercept the content of the communications but also to track the location of and gather other information about the participants. The digital age has also enabled the storage of immense amounts of data readily retrievable in response to infinite variations of search criteria. Data about individuals can be collected at the brick-and-mortar or online point of sale, when passing through toll booths equipped with license plate reader technology, from the use of digital wireless phones, from monitored communications, and from a growing universe of other sources. Data can be analyzed to reveal the most personal facts about a person's life.

Additionally, advances in technology have made possible sophisticated means of tracking a person's movements and capturing their electronic data. The range of devices and techniques available to governments is ever expanding as technology rapidly evolves. Often there is no physical intrusion into one's home, business or automobile, meaning that the invasion of privacy may now leave no detectable trace. The use of advanced means of data collection and surveillance may remain hidden from discovery by the individuals affected, their attorneys, and ultimately the courts in which they are eventually subjected to prosecution.

To address these new threats to privacy posed by the digital age, the National Association of Criminal Defense Lawyers, the Foundation for Criminal Justice, the American University Washington College of Law, and the *Criminal Law Practitioner* presented a symposium entitled "The Fourth Amendment and the Digital Age." We assembled an outstanding group of criminal law practitioners, academics, and leaders from the technology sector. Topics included an in-depth look at the high-tech surveillance and data collection methods currently in use and those coming on the horizon, the evolving Fourth Amendment law addressing these developing threats to privacy, and advanced litigation strategies for raising Fourth Amendment objections to these surveillance programs and techniques and the introduction of evidence derived from them.

As the technology available to governments evolves, so too must we understand its potential to invade privacy in ways never imagined by the drafters of the Fourth Amendment, but most certainly contrary to the limitations on government power that they envisioned. The defense bar must also be equipped to challenge the use of these practices through sophisticated litigation strategies. This symposium was an important step in furtherance of these objectives.



E.G. "Gerry" Morris, President

National Association of Criminal Defense Lawyers

Executive Summary

The Fourth Amendment has entered the digital age. New surveillance technologies — from GPS tracking devices to automated license plate readers to bulk data collection — have upended traditional law enforcement practices and created new challenges for defense lawyers. This symposium addressed three substantive areas of concern related to these technological and legal changes.

First, the symposium examined how the United States government is collecting, searching, storing, and sharing information on suspects and non-suspects alike.

The developments in surveillance technology are profound and troubling. Law enforcement and foreign intelligence analysts have shifted away from passive collection to an active collection strategy. Individuals and groups have been directly targeted, information collected and shared, and investigations expanded. Further, this active collection has been combined in the foreign intelligence context with bulk collection methods, sweeping up millions of records for later study. Mass surveillance has matched targeted surveillance as a tool of domestic security. These changes are extreme, involving intrusive interception, hacking, malware, and other surreptitious methods. While primarily targeting the foreign intelligence space, these tactics have continued to spill over to the domestic law enforcement side.

In the foreign intelligence context, the law has failed to catch up. In fact, the law has become rather permissive, allowing extensive intelligence collection without robust legal restrictions. Bulk metadata collection has been allowed under Section 215 of the USA Patriot Act. Broad sweeps of foreign communications content has been allowed under Section 702 of the FISA Amendments Act. Collection of signals intelligence, including overseas communication and metadata, has been allowed under Executive Order 12333. These changes are part of a larger expansion of foreign surveillance powers, the development of which raises new questions for lawyers defending individuals in criminal cases.

In the domestic law enforcement context, the transfer of funds to domestic counter-intelligence has encouraged new technologies to be used on local populations. Cell-site simulators capture phone calls, automated license plate readers track vehicles, and big data dossiers create risk profiles — all funded and largely inspired by technological successes arising from foreign surveillance practices. These new surveillance techniques, while developed for counterterrorism, have largely been used for non-terrorism-related investigations.

Domestic legal restrictions, rules, and policies have yet to adapt. The constitutional protections of the Fourth Amendment in the digital age remain unsettled. In fact, the growing proliferation of exceptions to the Fourth Amendment — from the third-party doctrine to the “foreign intelligence surveillance exception” — has largely undermined existing protections.

Faced with technological and legal challenges, the symposium called on defense lawyers to draw attention to the increased threats from surveillance and the gap in legal protection. In practice, this requires a public education campaign to explain the threat of new technology to the public, to translate the existing technology to lawyers, to publicize the abuse of surveillance technologies being used in criminal cases, and to engage the business community and the greater legal profession as partners.



The symposium's second theme involved how recent changes in Fourth Amendment doctrine and police practices have created opportunities and challenges for defense lawyers.

The symposium focused on two major Supreme Court decisions. *Riley v. California*² held that a warrantless search of a smartphone incident to arrest violated the Fourth Amendment. *United States v. Jones*³ held that long-term warrantless GPS monitoring was a search for Fourth Amendment purposes. Both cases required the Court to rethink its approach to digital information and surveillance. Both cases also present new litigation opportunities for criminal defense lawyers.

Specifically, the *Riley* case showcased the Supreme Court's first foray into considering how digital information and data storage devices (like smartphones) may be different than their physical, non-digital analogues. As more surveillance devices intercept digital information and as more personal devices contain digital information, a Fourth Amendment based on a non-digital world will need to adapt. *Riley* may well signal a break with precedent, allowing the argument that "data is different" to control the analysis. Similarly, high-tech surveillance devices like GPS trackers upend the traditional, physical restraints of time, effort, and resources required to track a suspect. In *Jones*, the Court wrestled with the implications of a growing surveillance apparatus, offering clues about how it might react to future Fourth Amendment challenges. The symposium panelists addressed this new reality and how the Fourth Amendment in a digital age might be more protective than the Fourth Amendment in the last few decades. While recognizing that defense lawyers must engage in pushing this argument forward, the panelists offered some cautious optimism about the first cases addressing these new technological challenges.

In addition to Fourth Amendment doctrine, the symposium addressed potential policy changes to curb growing domestic surveillance practices. Much of this change could be done on the federal level and responds to the increasing federal funding of local law enforcement through homeland security and counter-terrorism grants.

Specifically, the suggestions included ending secrecy agreements that preclude local governments from admitting that they are using new surveillance technologies. Two recent cases highlighted the fact that local law enforcement was under a secrecy agreement in the use of Stingray technology, such that they could not even admit its use in court. Similarly, a suggestion was made to ensure that the judiciary understands the technology that is being used for surveillance. One recent case demonstrated that judges had been regularly signing orders without actually understanding the technology behind the surveillance they had been approving. More generally, the suggestion was to require accountability in the use and monitoring of new technologies and to establish consistent federal policies for those technologies. Currently, the federal government largely shares the technology with local officials without sufficient accountability and without consistent policies.

The third topic of the symposium looked to the future, asking how the courts, Congress, and companies might adapt to the rise of the surveillance state.

Courts are responding to the challenges of the Fourth Amendment in a digital age as can be seen in the forward-thinking decisions in *Riley* and *Jones*. At the same time, the contours of *Riley* and *Jones* are unformed. Real questions exist about how the Supreme Court will apply these cases in the future. New technologies involving drones, pervasive audio and video surveillance, and biometric capture will present harder questions than those answered in the two decided cases. In addition, the exceptions to the Fourth Amendment — the administrative search doctrine, the third-party doctrine, and the national security exception — may continue to grow as well.



Congress is also responding to the challenge of the Fourth Amendment, although as the panelists conceded, final passage of new legislation may run into political difficulty. Proposals to amend the 1986 Electronic Communications and Privacy Act (ECPA) to require a warrant to obtain the content of communication data have received the support of a broad business coalition known as the Digital Due Process coalition. In addition, renewal of Section 215 of the USA Patriot Act may require changes to the legislative authorization of bulk collection. Other issues to be debated involve how Congress might regulate “the Internet of Things” and the growing use of end-to-end encryption.

Technology companies may also alter the legal landscape. Currently, private companies control much of the privacy protocols in place. Companies can share information with the government. Companies can insist on more formal, legal process before sharing information. In an international business context this can make for difficult decisions about openness, security, and law enforcement need. Technological responses such as encryption highlight the tension between security and law enforcement needs. The problem of “going dark” such that even a warrant cannot unlock encrypted data is a debate that continues today. In addition, the related tension of geo-locational privacy and content protection from wireless devices has yet to be addressed. The symposium panelists suggested that the focus on data protection, as opposed to data privacy, might reframe the future debate. They also suggested that the way forward involves new legislative oversight that responds to the constitutional, regulatory, and technological innovations already taking place.



Recommendations

Legal Strategy

- ⌚ Litigators should develop Fourth Amendment suppression strategies focused on new Supreme Court cases such as *United States v. Jones* and *Riley v. California*.
- ⌚ Litigators should utilize the newly rediscovered Fourth Amendment “trespass theory” that arises from Justice Scalia’s opinion in *Jones*.
- ⌚ Litigators should challenge all long-term and aggregated surveillance techniques, arguing that such collection of information is equivalent to a “mosaic theory search” recognized by the five concurring justices in *Jones*.
- ⌚ Defense counsel should identify cases in which older, pre-digital precedent no longer applies to the digital capture of information and should use *Riley* to suggest cases involving digital evidence be treated differently than cases involving non-digital evidence.
- ⌚ Lawyers should develop shared litigation strategies to challenge surveillance practices at the national and local level. Specifically, lawyers should share materials on how to litigate and challenge new technologies such as Stingray devices (or equivalent IMSI capture technologies).
- ⌚ Litigators should challenge the scope of authority for domestic surveillance. The blurring of foreign surveillance into domestic law enforcement must be policed.

- ☞ Defense lawyers have a new obligation to seek discovery about the source of law enforcement information to determine if the prosecution has exploited new (and sometimes secret) surveillance technologies.
- ☞ Litigators must develop a sustained challenge to the existing third-party doctrine that removes significant Fourth Amendment protections of personal data. Organizations, bar associations, and academics must support this challenge to reconceive how personal data is considered for Fourth Amendment purposes.

Education

- ☞ A national campaign to educate the public about the growth of the surveillance state needs to be articulated and funded. Citizens have not been engaged in the debate because most of the developments have been hidden. This project should promote the ideas of technologists, legal scholars, and institutions that have identified constitutional threats to privacy and liberty.
- ☞ A parallel educational project needs to be developed to educate judges about how to think about new technology. An education program should include programs for judges to learn about existing technologies.
- ☞ Lawyers need to educate themselves about the technology underlying these new surveillance techniques. In addition, lawyers must be sufficiently conversant with these techniques to effectively litigate the issues in court. Bar groups should begin lawyer-focused education programs to engage colleagues in re-examining the source and authority of government intelligence.

Legislative Advocacy

- ☞ The defense bar should play a key role in shaping legislative changes by providing stories about how new digital searches and technological surveillance are being implemented on the ground. Many of the proposed laws have been shaped by criminal cases or news stories.
- ☞ Encourage partnerships with businesses that have the capacity to create technological solutions and also have the financial resources and political capital to influence legislation.
- ☞ Consider both state and federal legislative remedies. State and local legislatures have acted to curb surveillance techniques, so the focus should not be limited to congressional action.

Policy

- ☞ End federal secrecy agreements. Federal policy should prohibit the federal government from demanding that states and localities hide the use of new surveillance technology. Requiring secrecy in order to receive new digital surveillance tools is unnecessary and undermines accountability and oversight.



- ☞ Require adherence to standards and accountability to the federal government on the part of local governments seeking to use new technologies financed by the federal government. Currently, the technologies are provided without accountability mechanisms to ensure they are used as intended.
- ☞ Require the federal government to adopt consistent policies to cover the use of new technologies. Currently, many technologies (e.g., the Stingray device) are provided without any standard operating policies.
- ☞ Promote technological solutions like encryption. While encryption is a contested topic — pitting technologists interested in data security against law enforcement interested in data access — it also provides a solution to government surveillance. As encryption becomes easier to use, the hope will be that protections of personal data will increase. Thus, even if the law (or courts) cannot catch up with data security, the technology might offer a solution.
- ☞ Refocus the problem of privacy as one of data protection. A data protection focus asks what individuals can do to control the data already collected, whereas a privacy focus asks how data is being collected. This distinction is central to the surveillance debate in Europe and might be helpful to the ongoing discussions in America.
- ☞ Require notice of the origin of the evidence in all criminal cases. Defendants should have the right to know what program or technology collected the evidence being used against them.



Symposium Overview

Dean Claudio Grossman, *Dean of American University Washington College of Law and the Raymond I. Geraldson Scholar for International and Humanitarian Law*

Theodore Simon, *President, National Association of Criminal Defense Lawyers*

New surveillance technologies threaten to distort Fourth Amendment doctrine and undermine individual privacy. On April 3, 2015, NACDL and the Washington College School of Law at American University hosted a symposium — “The Fourth Amendment in the Digital Age” — to address these new legal and technological challenges. The symposium assembled a distinguished group of technologists, law professors, lawyers, and policy advocates to identify and discuss legal issues arising in the digital age.

The symposium focused on three major issues: (1) new developments in surveillance technology; (2) potential legal strategies to challenge these new technologies; and (3) future legal and policy changes that could be made to address these new technologies. In addition, the symposium hosted a luncheon conversation between Joseph P. Nacchio, former Chairman and CEO of Qwest Communications International, and Norman L. Reimer, Executive Director of NACDL.

The symposium attracted practitioners, law professors, students, and the media to address critical and contested constitutional issues. The entire symposium was broadcast on C-Span, and reporters from the *Washington Post* and other news outlets were in attendance.

Two themes emerged as dominant issues throughout the day-long discussion. First, many panelists recognized that the Supreme Court has signaled an openness to treat digital information as qualitatively different from other personal property in recent cases. In addition, the Supreme Court appears to acknowledge that invasive surveillance techniques might alter fundamental privacy values and personal relationships, although it has not agreed on how to define or determine appropriate limits. While largely unsettled as a matter of doctrine, many commentators were hopeful that recent Supreme Court decisions would lead to a continued expansion of Fourth Amendment protections. Second, because of the unsettled doctrine, many commentators also looked to technological or legislative fixes that could supplement constitutional protections. While panelists differed in their optimism for the future, the possibility of creating a more protective legal structure for digital surveillance remained a familiar refrain throughout the symposium.

The symposium began with opening remarks by Dean Claudio Grossman and NACDL President Theodore Simon.*

Privacy as a Human Right

Claudio Grossman, Dean of American University Washington College of Law and the Raymond I. Geraldson Scholar for International and Humanitarian Law, welcomed the assembled group, thanking the sponsors and organizers of the symposium.

Dean Grossman reminded the audience that privacy is a human right, recognized by the international community and protected by international conventions. The threat posed to privacy by new surveillance capabilities must be considered also as a threat to human rights.

*Titles in the report are reflective of the time of the Symposium. E.G. “Gerry” Morris is currently President of NACDL.



Dean Grossman described the symposium as symbolizing a recognition of human dignity and the rule of law, and commended NACDL for consistently upholding those values. He emphasized the importance of partnering with organizations like NACDL and looking outward to the world community for inspiration. Because domestic privacy protections in the United States have remained largely underdeveloped, Dean Grossman suggested a more internationalist approach to the privacy problem, explaining that international human rights law and international agreements provide a better analytical framework to analyze privacy as a human right than existing constitutional norms.

Technology has provided opportunities to have access to information, to share information, to provide support and communicate to those who would have been isolated in a different situation. However, technology is also vulnerable and technology can create big problems in terms of human rights. We are more vulnerable to electronic surveillance and interception and recent discoveries have revealed how the technologies that are being developed currently often facilitate practices with chilling efficiency.

Claudio Grossman

Dean Grossman concluded with a word of caution about the double-edged nature of technology in the human rights context. "Technology has provided opportunities to have access to information, to share information, to provide support and communicate to those who would have been isolated in a different situation. However, technology is also vulnerable and technology can create big problems in terms of human rights. We are more vulnerable to electronic surveillance and interception, and recent discoveries have revealed how the technologies that are being developed currently often facilitate practices with chilling efficiency." This duality requires consistent attention by lawyers and advocates involved in the human rights struggle. He noted that we have seen the impact of the erosion of human rights around the world, while at the same time the international community has been able to organize the use of new technologies to protect human rights. From that perspective, the subject of the symposium is a valuable contribution to the cause of human rights and an important topic to cover.

Dean Grossman introduced Theodore Simon, President of NACDL.

The Fourth Amendment as Protest

On behalf of NACDL, Mr. Simon welcomed the group to the symposium. Mr. Simon described the goals of the symposium as examining how new technologies will effect criminal cases and how criminal lawyers can shape the law.

Mr. Simon reflected on his own career as a criminal defense attorney that began fifty years ago at American University. He contrasted the turbulence of the street protests of 1967 with the legal protests made today in court. He remarked, "Today, as lawyers, our protest arises through proactive litigation and motions to suppress." This protest has found its main source in the Fourth Amendment, and those privacy and security freedoms are more at risk than ever before. As technology and surveillance capabilities have expanded, constitutional protections have weakened and the ability to protest has waned.



Mr. Simon acknowledged, however, that new Supreme Court cases, most notably *Riley v. California*,⁴ provide a breath of fresh air for those concerned about Fourth Amendment protections. *Riley*, he argued, may signal a strengthening of Fourth Amendment rights and a recognition of real privacy interests in personal communication devices. This recognition was a first for the Supreme Court and portends a potentially far-reaching precedent. While concerns exist about a weakening of constitutional remedies, the specific issue of rights in the digital age appears to be a bright spot.

Mr. Simon stated that today, issues surrounding technologies strike at the heart of the Fourth Amendment. These changes pose new challenges for criminal defense lawyers and create a new urgency to make sure that technology allows for transparency and accuracy. Mr. Simon proposed that advocates push to update the surveillance laws to address new technologies, recognizing the unique role criminal defense advocates can play to ensure an appropriate balance between liberty and technology. A combination of legislative change and continued Fourth Amendment litigation is the only way to preserve Fourth Amendment freedoms in a digital age. Mr. Simon concluded by proclaiming that this a transformational moment in the law, a moment in which “liberty hangs in the balance.”

1. New Developments in Surveillance Technology: How the Government Collects, Searches, Stores, and Shares Information

MODERATOR:

Professor Jennifer Daskal, Assistant Professor of Law, American University Washington College of Law

DISCUSSANTS:

Catherine Crump, Assistant Clinical Professor of Law; Associate Director, Samuelson Law, Technology and Public Policy Clinic, UC Berkeley School of Law

Elizabeth Goitein, Co-Director of the National Security Project, Brennan Center for Justice at NYU School of Law

Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology

Eric Wenger, Director of Cybersecurity and Privacy Policy for Global Government Affairs, Cisco Systems

There has been a tectonic shift in the way data is collected and stored and the ways in which we communicate over the past ten, fifteen years.

Jennifer Daskal

Professor Jennifer Daskal introduced the panelists and opened the session by commenting on the rapid change in how data is collected and analyzed. As Professor Daskal stated, “I’m going to remind us of what we all know, that there has been a tectonic shift in the way data is collected and stored and the ways in which we communicate over the past ten, fifteen years. So the panel is going to explore the implications of what has happened and what it means for law and policy.”

Developments in Surveillance Technologies

As an initial question, Professor Daskal asked Joseph Lorenzo Hall, as the technologist on the panel, to explain the underlying technological changes that have occurred. She asked, “What is the world we are living in? What has changed in the past 10-20 years?”



Mr. Hall detailed three major shifts in surveillance technology: (1) a move from passive collection to active collection; (2) a move from targeted collection to bulk collection; and (3) a move to more intrusive methods of surveillance.

Passive to Active Collection

As to the first shift from passive collection to active collection, Mr. Hall described how the traditional forms of passive collection like eavesdropping are being replaced by new methods of more aggressive collection. Traditional forms of surveillance used to involve situations in which someone was communicating and law enforcement could sit and capture the information and analyze it. The new methods are characterized by proactive surveillance, whereby law enforcement is interfering with the communication flow in order to reach out and access the data. As an example, Mr. Hall pointed out that when customers communicate with their bank online, they see a little lock icon on the screen. This lock icon symbolizes that the communication is secure, encrypted, and validated. However, technology now exists to allow for law enforcement to get between the customer and the bank. These attacks, called “man in the middle attacks,” can reveal personal information. Essentially, what happens is that signals can be sent to pretend that the person doing the surveillance is actually the authorized person meant to receive the message. By fooling the system into believing it is communicating with an authorized sender, law enforcement can infiltrate a computer system and observe the communication flows. Obviously, such surveillance will undermine trust in the larger communication system, but it can provide valuable information. Mr. Hall also mentioned another example of an active attack called QUANTUM — a global targeting attack method that can intervene in one’s communication tools (essentially poke a hole in a browser) to capture key strokes, passwords, and spy on the user.

Targeted Collection to Bulk Collection

As an example of the move from targeted collection to bulk collection, Mr. Hall described a program called MUSCULAR, which allowed the National Security Agency (NSA) to essentially tap the data links between Yahoo and Google data centers and collect all of the information sent over those links. The NSA had access to everything, sweeping up more information than the agency could possibly use. The additional problem, of course, was that approximately 99.9 percent of the individuals were absolutely innocent of any wrongdoing and yet, the NSA had it all. As Mr. Hall stated, “They were basically collecting all the hay in the haystack to get access to however many needles were in the haystack.”

Unintrusive Methods to Intrusive Methods

Finally, Mr. Hall stated, “[t]his kind of surveillance has gone from relatively unintrusive [part of this is just how society has evolved] to very intrusive. . . . You get this combination of sophisticated analytical techniques and then subversion of technical hardware and software. . . . And then there are other things like cohort analysis where people on the same train with a target may be implicated as well. You know, we are all creatures of habit [I see the same people on my train all the time] and so there is a big opportunity for false positives — identifying someone for suspicion that shouldn’t have that suspicion.” Sophisticated collection technology and cohort analysis now allow new inferences to be drawn and suspicions to be created from personal data. In addition, increasingly sophisticated software and hardware will allow easier attacks on encryption. As but one example, the NSA intercepted Cisco products while they were en route to their destination without Cisco’s knowledge. These products were then modified to allow the NSA access to ordinary consumer products, undermining the security and integrity of the products.⁵ This type of intrusion built right into the hardware of the technology marks a new form of surveillance.



0110

0100

0011

1001

1010

1100



0111

0011

0101

1001

0000

1110

0110

1011

0010

0001

1100

1101

Developments in the Legal Framework

Professor Daskal then asked Elizabeth Goitein to describe the legal framework for foreign intelligence surveillance and explain whether it has kept up with the technology.

The legal distinction between collecting information at home and collecting information overseas has really become a legal fiction given the way digital data is transmitted and stored.

Elizabeth Goitein

A Permissive Legal Framework for Collection

Ms. Goitein began by acknowledging that technology has made it much easier to target data — including data of American citizens. She explained that while the logical response to sophisticated technological change might be to fortify the protections of personal data, in fact, the actual response has been the exact opposite. In contrast to the 1970s, after revelations from the Church Committee⁶ resulted in the development of laws and policies forbidding intelligence agencies from gathering information without individualized suspicion, after September 11th, the focus on individualized suspicion has been “jettisoned from the law.” To illustrate, Ms. Goitein focused on three legal authorities that shifted from more tailored to mass surveillance, and weakened the legal framework for collection.

Section 215⁷ and Metadata

Section 215 of the Patriot Act⁸ currently allows the government to get a FISA court order compelling companies to turn over business records, including phone records. Before 9/11, the standard required that the government demonstrate that the subject of the records was a foreign power or an agent of a foreign power. The Patriot Act amended the law so that the government now does not have to show anything about the subject of the records, but only that the records themselves are “relevant” to the investigation. Further, the FISA court interpreted “relevance” to mean that millions of telephone records can be collected if there are relevant records buried somewhere within these records. The consequence is that records can be collected in bulk without any individualized suspicion.

Section 702 and Communications Content

Section 702 of the FISA Amendments Act,⁹ which relates to the collection of communications content and metadata from calls and emails between Americans and foreigners overseas, has provided broader access to that communications data. Before the FISA Amendments Act, the government was required to show probable cause to the FISA court that the target of the surveillance was a foreign power or its agent, which, for an American, is defined in a way that implicates criminal activity. In 2007¹⁰ and 2008,¹¹ Congress amended the law to get rid of any requirement for an individualized court order when the communications are between an American and a foreign target and the information is for foreign intelligence purposes. The target no longer needs to be a foreign power or agent of a foreign power. The target only need be a foreigner abroad. Again, we have moved from essentially something that required a warrant to mass collection with no suspicion of wrongdoing.

Executive Order 12333 and Signals Intelligence

Executive Order 12333¹² allows for the overseas collection of signals intelligence, including communications content and metadata. This Executive Order is the most expansive of the government's foreign intelligence surveillance authorities, and it never contained a requirement of individualized suspicion. The Executive Order allows agencies to collect foreign intelligence, defined to include any information about the activities of foreign persons, with the understanding that incidentally obtained U.S. person data would be "minimized" unless it included foreign intelligence or evidence of a crime. What has changed here is not the legal constraints but the practical ones. The limits on data storage and analytical capacity have nearly vanished. Also, as data travels internationally, it becomes confusing and ineffectual to rely on territorial limitations for protections. As Ms. Goitein concluded, the "legal distinction between collecting information at home and collecting information overseas has become a legal fiction given the way digital data is transmitted and stored." The notion that Americans have no constitutional interests at stake when the NSA taps into data centers in Europe no longer makes sense.

The Business of Surveillance

Professor Daskal asked Eric Wenger, "What are the resulting perceptions around the world and the implications for US business? Has the government's response been adequate?"

Issues of Security and Trust

Mr. Wenger acknowledged that Cisco is working on issues of security and trust in the surveillance context. The difficulty, of course, is that there are things companies cannot control. Customers operate products within networks, and many times the security is jeopardized by nation-state to nation-state attacks.

From a business perspective, Mr. Wenger acknowledged the difficult challenge in balancing governmental powers, transparency around the use of those powers, and the need to have a dialogue about those powers. He said, "At Cisco, we don't view privacy and security as a zero-sum game. They are clearly connected. At the same time we don't view economic growth as being something separate from national security. They

Economic growth depends on trust. It's hard to quantify damage but I think if you look at some of the examples that we have talked about you see significant expenditures by US companies that can serve as a pretty good proxy for measuring the scope of the problem. . . . You also see companies making efforts to build data centers in a way that allows for localization, putting data closer to their customers. Some of that may be based on performance but some of it is based on satisfying concerns that customers might have about where their data is stored and what laws are used to protect that data and that's all expensive. Trust has clearly been impacted for companies across the technology industry, including Cisco.

Eric Wenger



Technologies invented for terrorism investigations were also put to use in ordinary law enforcement. Stingray devices, which replicate a cell phone tower in a way that allows for wireless cell phone tracking, have been purchased for terrorism investigations but are used for ordinary drug crime investigations. Automatic license plate readers are now able to track automobiles in a city, and facial recognition technologies will be able to track individuals.

Catherine Crump

are intertwined.” He recognized that “[e]conomic growth depends on trust. It’s hard to quantify damage but I think if you look at some of the examples that we have talked about you see significant expenditures by US companies that can serve as a pretty good proxy for measuring the scope of the problem. . . . You also see companies making efforts to build data centers in a way that allows for localization, putting data closer to their customers. Some of that may be based on performance, but some of it is based on satisfying concerns that customers might have about where their data is stored and what laws are used to protect that data, and that’s all expensive. Trust has clearly been impacted for companies across the technology industry, including Cisco.” Companies such as Twitter and Yahoo have pushed back on government requests for customer data.¹³ Microsoft is litigating against the US Attorney’s Office in New York over data stored in Ireland.¹⁴ Other cases are being litigated around the country.

Business, Security, and Law

As a related matter, certain business decisions, such as where to locate data centers, may be influenced by local laws and surveillance demands. Companies need to protect their data and thus they are looking for safe places to store it. Potential new surveillance technologies or aggressive laws have impacted the trust companies strive to build and the business brands they try to promote. For customers, the focus must be on security against nation-state attacks in addition to more traditional attacks by criminal elements. Thus, Mr. Wenger argued, going forward we need to have a dialogue between governments about what is acceptable because the sophistication of the actors is growing greater than the resources of any particular technology company.

Surveillance and Local Law Enforcement

Professor Daskal asked Professor Catherine Crump, “We have been talking a lot about foreign surveillance. But what are you seeing in terms of changes in law enforcement? What kinds of new technology are being used and for what purposes, with what kinds of implications?”

Local Surveillance

Professor Crump began by focusing on most people’s everyday interaction with local law enforcement. First, she commented that it is important to remember that local law enforcement was also impacted by the post-9/11 changes. The targeting of homegrown terrorism and the transfer of funds to domestic counterintelligence created new surveillance technologies available on a local level. Because there was money to secure ports, cities like Seattle purchased drones from a “port security grant.” Because there was money for border security, non-border states adopted border security technologies. These technologies, of



course, may capture individuals doing criminal acts that are neither terroristic acts nor violations of national security. But, because the technology was available, local law enforcement purchased and implemented it. Other technologies invented for terrorism investigations were also put to use in ordinary law enforcement. Stingray devices, which replicate a cell phone tower in a way that allows for wireless cell phone tracking, have been purchased for terrorism investigations but are used for ordinary drug crime investigations.¹⁵ Automatic license plate readers are now able to track automobiles in a city, and facial recognition technologies will be able to track individuals.¹⁶

I think there is a double problem here. First of all, uses of these technologies have been themselves shrouded in secrecy and criminal defense attorneys can't file suppression motions when they don't know that the evidence was gathered in a way that might be amenable to that.

Catherine Crump

Litigating Surveillance at the Local Level

"I think there is a double problem here. First of all, uses of these technologies have been themselves shrouded in secrecy and criminal defense attorneys can't file suppression motions when they don't know that the evidence was gathered in a way that might be amenable to that." Professor Crump ended by suggesting that a strategy should be developed to share materials on how to litigate these issues and craft arguments that will appeal to judges to oversee new surveillance challenges.

There is something called the "third-party doctrine," which says that any information that you voluntarily disclose to a third party, you do not have a reasonable expectation of privacy in that information.

Elizabeth Goitein

Regulating Surveillance with the Fourth Amendment

Professor Daskal turned to Elizabeth Goitein and Catherine Crump to ask, "What are the limits in terms of relying on the Fourth Amendment to regulate for both foreign intelligence surveillance and law enforcement collection?"

Foreign Intelligence Surveillance

Ms. Goitein discussed three relevant limitations on how the Fourth Amendment applies. First, she discussed the foreign intelligence exception to the warrant requirement. In the 1970s, federal appeals courts determined that the government did not need a Fourth Amendment warrant to collect foreign intelligence, but placed strict limits on the exception — for instance, the target had to be a foreign power or its agent. The FISA Court, however, has discarded all these limits. The Supreme Court has not decided whether there is a foreign intelligence exception, so there is legal uncertainty here. Second, some have argued that the



0110
0100
0011
1001
1010
1100

government does not need a warrant to collect the communications of a foreigner overseas, and that this authority automatically extends to the people with whom the target is communicating. The case law, however, does not support this argument, because it addressed situations where the government did obtain a warrant for the target and implemented very strict minimization requirements.¹⁷ Finally, Ms. Goitein explained that the FISA Court has held that bulk collection of Americans' telephone records does not constitute a search for Fourth Amendment purposes because the information about who we call is information we share with a third-party. "There is something called the 'third-party doctrine,' which says that any information that you voluntarily disclose to a third-party, you do not have a reasonable expectation of privacy in that information."¹⁸ Ms. Goitein noted that this doctrine has come under attack and probably will not last long, as it does not match up with the realities of life in the digital era.

Mr. Wenger remarked that the Microsoft case is a modern example of the tension raised by the third-party doctrine's application to foreign law.¹⁹ In that case, the government had subpoenaed phone records of companies in the United States even though the data at issue was located overseas. The government's position, however, has been that since the customer records belonged to the provider, the third-party doctrine entitles the government to get access to it without a warrant. The companies, in response, argued that the data is in a foreign data center and that the government's subpoenas are limited by the territorial power of the United States. Since the warrant is requesting data outside the US and outside the US subpoena power, then the third-party doctrine should not apply. However, Mr. Wenger also commented on the legal and practical justifications for why the third-party doctrine exists. He distinguished between the records of a transaction and the communications themselves, explaining that sometimes businesses had to monitor the transactions. For example, a bank cannot transfer money unless it knows the accounts from which the money is coming and where it is going. The transfer record thus belongs to the bank, and it should have a right to collect it. All bank customers know this reality, and thus it remains difficult to understand why there should be an expectation of privacy in the transfer information.

The Snowden revelations also allowed companies to push back against the government in terms of collection. This reality, combined with the Supreme Court's decision in *Riley*, has provided some optimism for civil libertarians concerned about government surveillance. At the same time, there is a concern about Fourth Amendment remedies. The rights will matter little if there can be no remedies for unconstitutional actions.

Catherine Crump

The Metadata/Content Distinction

The debate continued between Ms. Goitein and Mr. Wenger about whether the distinction between metadata and content can really hold in an era in which metadata can be quite revealing. For example, if someone calls a suicide hotline and hangs up, there may be no content but the call itself is quite revealing. Mr. Wenger countered that while good policy arguments support Ms. Goitein's position, the law still makes that distinction between communications and the content of the communications. Further, definitional issues were raised by Mr. Hall, who questioned whether the distinction between U.S. persons and other persons can hold if neither the target's location nor identity can be identified with precision. As Mr. Hall explained, the reality is that network geography — the topology of the internet — makes it difficult to

understand how data travels. A packet of information might go around the world, to go down the street. As such, political and geographical geography do not map well. Similarly, identity is hard to pin down. Usually, the NSA will assume that the target is not in the US and work backwards, an assumption that allows the NSA greater access to information.

Professor Crump brought up the role of Edward Snowden as a figure who has changed the discussion of the surveillance debate. In addition to providing some transparency about the technologies in existence, the Snowden revelations also allowed companies to push back against the government in terms of collection. This reality, combined with the Supreme Court's decision in *Riley*, has provided some optimism for civil libertarians concerned about government surveillance. At the same time, there is a concern about Fourth Amendment remedies. The rights will matter little if there can be no remedies for unconstitutional actions.

The technology is both complicated and always changing, and lawyers, including judges, remain relatively uniformed.

Joseph Lorenzo Hall



Challenges Going Forward

Translating Technology for Lawyers

Mr. Hall responded that he saw two main challenges ahead. First, he explained the need to get information to lawyers about these technological changes. Part of that challenge is to find out what information exists and what law enforcement agencies are actually doing. Leaked PowerPoint slides or FISA releases do not provide a transparent window into the existing collection mechanisms. This secrecy results in lawyers being unable to examine or challenge these surveillance methods in court. The second challenge is that it is very hard to teach lawyers how network operations and network security work. The technology is both complicated and always changing, and lawyers, including judges, remain relatively uniformed.

Explaining the Threat to the Public

Ms. Goitein responded that a major challenge is getting the public to see that the threat exists. The potential for abuse of surveillance technology is real, and many Americans do not see the threat. The pull of American Exceptionalism, the idea that somehow our government will not use its national security powers against the people even though history is full of examples of such abuses by this country as well as others, is a strong force. In addition, the technology advances so quickly that public opinion cannot keep up and the law lags even farther behind. Finally, the central function of today's intelligence establishment is to collect and use data on a massive scale. Changing the status quo is therefore not just about changing the law, but breaking down and redefining institutions, and there are huge institutional forces arrayed against such change.

Defining Legal Authority

Mr. Wenger stated that one of the problems going forward is the scope of authority of the US government to collect metadata information and to target communications of people in the United States. He argued that we need to figure out the scope, the procedures, and rules of the road. In addition, Mr. Wenger stated that we must do so outside the existing domestic statutes in place. Many companies

work and do business outside the United States. The protection of domestic persons is important, but it is cold comfort to non-US persons. As such, technology companies must look outside of that space to the international context.

For far too long the government, the executive specifically, has been able to engage in extremely aggressive surveillance programs with little public knowledge and with real harms as a result.

Catherine Crump

Publicizing Surveillance Technology

Professor Crump posited that “for far too long the government, the executive specifically, has been able to engage in extremely aggressive surveillance programs with little public knowledge and with real harms as a result.” The example of the Stingray cell phone catcher — a device that has been in use for at least a decade — is only now being litigated by criminal defense lawyers. This type of secret technology must be revealed and exposed. In addition, new technology-focused bills have been introduced on the state and local levels, which represents another area of optimism in the face of otherwise encroaching technology.

2. Challenges to the System: Prosecutors, Judges, and Defense Attorneys in the Digital Age

MODERATOR:

E.G. “Gerry” Morris, *President-Elect, National Association of Criminal Defense Lawyers*

DISCUSSANTS:

Hanni Fakhoury, *Senior Staff Attorney, Electronic Frontier Foundation*

Neema Singh Guliani, *Legislative Counsel, American Civil Liberties Union*

Jim Harper, *Senior Fellow, CATO Institute*

Orin Kerr, *Fred C. Stevenson Research Professor of Law, George Washington University Law School*

Tactical Challenges to New Technologies in Court

E.G. “Gerry” Morris, co-chair of NACDL’s Fourth Amendment Committee and NACDL President-Elect, introduced the second panel, which discussed what can be done about new surveillance techniques and how lawyers can challenge these technologies in court. The panel shifted focus from a discussion of the developing technology to a discussion of legal tactics to challenge that technology.

Mr. Morris asked the panel to examine three main questions. First, what is the current Fourth Amendment law regarding issues of digital technology? Second, where is the Fourth Amendment going with these types of technological challenges? And third, how can lawyers know that any surveillance technology was, in fact, used in their individual cases?

The good news is that the Supreme Court has been rather creative in interpreting the Fourth Amendment when it comes to new technologies.

The bad news, however, is that the Supreme Court has narrowed the exclusionary remedy available for violations of constitutional rights.

Orin Kerr

A Good News/Bad News Update

Professor Orin Kerr began by explaining there was good news and bad news with respect to current Fourth Amendment law concerning new technology. The good news is that the Supreme Court has been rather creative in interpreting the Fourth Amendment when it comes to new technologies. In *Riley v. California*, for example, the Court required a broad warrant requirement to search a cell phone incident to arrest.²⁰ This trend, Professor Kerr argues, opens an opportunity for defense lawyers to develop creative arguments around new technologies. He called this the “the *Riley* Moment” and suggested that lawyers look for “*Riley* Moments” in their cases.

The bad news, however, is that the Supreme Court has narrowed the exclusionary remedy available for violations of constitutional rights. The Supreme Court has chipped away at the exclusionary rule in cases like *Davis v. United States*, diminishing the availability of the suppression remedy.²¹ So, even if rights expand, for practicing criminal defense lawyers who need exclusionary remedies for their clients, the results in criminal cases may well be the same.

Professor Kerr commented that these trends are related. As the Supreme Court narrows application of the exclusionary rule, it becomes more comfortable creating a broader understanding of rights because defendants are not actually getting out of jail. Put simply, Professor Kerr stated, the good news is that Fourth Amendment rights are expanding, but the bad news is that accused persons will not benefit from this expansion.

Litigating Jones

For defense attorneys there are new cases that have redefined searches or seizures under the Fourth Amendment. Lawyers should be relying on the “trespass theory” that arises from Justice Scalia’s majority opinion in *United States v. Jones*.²² While courts and commentators are not exactly sure what *Jones* means in practice, they do know that there is a new trespass/physical intrusion theory that needs to be litigated. In addition, in *Grady v. North Carolina*,²³ the Supreme Court held that *Jones* applies to persons. In *Grady*, the State of North Carolina attached an ankle bracelet with GPS monitoring around a person’s ankle without a warrant. The Supreme Court held this was a Fourth Amendment search because the bracelet physically intruded on the subject’s body and was designed to obtain information. In addition, the concurring opinions in *Jones* also departed from and expanded traditional Fourth Amendment conceptions of persons in public. Long-term and aggregated GPS monitoring over time is now a Fourth Amendment search because of the extent of the information revealed. This insight should be helpful whenever there is a digital collection of evidence. Many times such digital collection is part of a broader effort to collect evidence, which can be used to create a mosaic of information about an individual. Under the *Jones* concurrences, this mosaic of information could constitute a Fourth Amendment search.



***Riley* and the recent cases provide new options to challenge the old Fourth Amendment doctrine, which is an exciting opportunity for litigation.**

Orin Kerr

Litigating Riley

In terms of Fourth Amendment reasonableness, Professor Kerr emphasized that defense lawyers can use *Riley* to suggest that cases involving digital evidence should be treated differently than cases involving non-digital evidence. Professor Kerr suggested lawyers look for “*Riley* Moments” in which the traditional non-digital precedent could be reworked to account for digital realities. Lawyers should be pushing for “*Riley* Moments” to argue that the traditional Fourth Amendment analysis should not control in these new digital cases. *Riley* and the recent cases provide new options to challenge the old Fourth Amendment doctrine, which is an exciting opportunity for litigation.

Rethinking Privacy and the Fourth Amendment

Jim Harper presented an alternative method to litigate Fourth Amendment issues in court. He suggested that lawyers emphasize privacy as the central condition that stands independent of “the reasonable expectation of privacy” test. Privacy exists without the Fourth Amendment, and the current two-pronged, reasonable expectation of privacy test derived from *Katz* has largely been a failure. Mr. Harper pointed to three specific failures in application. First, courts rarely analyze the subjective prong in the *Katz* test, and the objective prong, in reality, tends to reflect the subjective opinion of particular judges. Second, the outcomes from applying *Katz* run counter to what ordinary people see as their reasonable expectations of privacy. Studies show that ordinary people’s expectations diverge from the intuitions of judges. Third, as a textual matter, the reasonable expectation of privacy test is not really the holding of *Katz* but merely the solo concurrence of Justice Harlan. The majority opinion in *Katz* turned on the fact that the defendant went into a phone booth and concealed his voice from the access of others. Mr. Harper predicted that the *Katz* test will soon be replaced, and he offered a new way to conceptualize arguments about the Fourth Amendment.

A Statutory Reading of the Fourth Amendment

Mr. Harper suggested that the best way to interpret the Fourth Amendment is how one might analyze any other law. Mr. Harper suggested that lawyers read the Constitution like any other statute, and follow the plain language of the document. Reading the text of the Fourth Amendment, first lawyers would ask whether there was a seizure or a search. Second, they would ask whether the thing seized or searched is protected by the Fourth Amendment. Then they would ask whether the search or seizure was reasonable.

Mr. Harper explained that *Jones* is actually a good seizure case to examine. The Supreme Court used the term “search,” but the Court was really talking about an invasion of a property right. Property rights go beyond the possession of a thing and include the use and benefits of a thing and the right to exclude. Viewed this way, the Fourth Amendment should focus on the right to be secure, including the right to exclude others. These are all part of the bundle that forms our property interest in our persons, papers, homes, and effects. Attaching a GPS device to the car converts the car to someone else’s use, and thus deprives the owner of the full rights to the car and invades the individual’s property rights. The car was seized under this theory because the car had been converted to the use of the government agents.

Mr. Harper observed that searches and seizures are often mixed, but that searches can happen separately. For example, in *Kyllo v. United States*,²⁴ a thermal imaging device was able to access the heat profile of the side of a home. The device made perceptible things that were otherwise imperceptible to the human eye. The Court held that this action was a search. There are alternatives about how to analyze a search, but by being granular and scientific one can answer the question rather simply. The search in *Kyllo* was a search because the thermal imaging machine allowed the police to see something they couldn't otherwise see.

As to the second question of what is protected by the Fourth Amendment, Mr. Harper argued that we should look to the language of the Constitution. In *Jones*, a car is an effect — property owned by the user. The constitutional language protects persons, homes, papers, and effects.

And then the question finally is — was it or was it not reasonable. And this is where the judgement happens and judgement has to happen; there is no test for the Fourth Amendment that gets away from it. But at least then the question is focused in the right place, which is on whether or not the government was being reasonable when it searched. The way the reasonable expectation of privacy doctrine works is that it examines whether the individual was being reasonable in expecting privacy and that's not what the terms of the Fourth Amendment call for.

Jim Harper

"And then the question finally is — was it or was it not reasonable. This is where the judgement happens and judgement has to happen; there is no test for the Fourth Amendment that gets away from it. But at least then the question is focused in the right place, which is on whether or not the government was being reasonable when it searched. The way the reasonable expectation of privacy doctrine works is that it examines whether the individual was being reasonable in expecting privacy and that's not what the terms of the Fourth Amendment call for." The emphasis matters because the Fourth Amendment was enacted to protect against unreasonable government actions, not to dictate reasonable expectations of the people. Generally, the reasonable expectation of privacy standard inverts this understanding, and Mr. Harper suggests a more historically grounded approach.

This is a way to administer the Fourth Amendment that's sound, that doesn't rely on the objective whims of judges in a given situation, and over time could restore the strength of the Fourth Amendment, applying it on its terms and consistent with precedent to new technological circumstances.

Jim Harper



0110

0100

0011

1001

1010

1100



0111

0011

0101

1001

0000

1110

0110

1011

0010

0001

1100

1101

A Statutory Application of Fourth Amendment Principles

To apply this statutory approach, Mr. Harper argued that one needs to understand how technologies work. He looked at the development of older communication technologies — paper, mail, wiretaps, sound waves, telephone communications, and the Internet. In each of these cases, the communications were secure and protected because they were the property of the individuals as the messages went in transit to the intended recipients. While surveillance techniques could intercept the message, the message was still the property of the speaker. Further, in each of the cases, the imperceptible information became perceptible only by the use of new surveillance technologies, leading to the conclusion that this interception was the search. “This is a way to administer the Fourth Amendment that’s sound, that doesn’t rely on the objective whims of judges in a given situation, and over time could restore the strength of the Fourth Amendment, applying it on its terms and consistent with precedent to new technological circumstances.”

Right now we have a bizarre tension happening at the federal level. On one hand, we are completely unable to keep pace with the technology development. . . . When we look at some of the issues that have arisen in recent months, it really involves technology that’s almost decades old. And I am pretty certain that there are other technologies that are either in the pipeline or even being deployed that we don’t even know about yet and we haven’t even had the opportunity to have a congressional or public debate about. And at the same time that we have . . . this complete inability at a federal level to put in place privacy protections or civil liberties protections regarding the use of these technologies, the government is awfully good at getting these technologies out into the hands of state and local law enforcement. . . . There’s not really a sufficient oversight and sufficient action by the federal government to make sure that these technologies are used responsibly.

Neema Singh Guliani

Federal Impact on Local Surveillance

Neema Guliani next addressed how current federal law and policy is impacting the technologies used by state and local law enforcement, including how these policies create barriers to challenging the technologies in court. As an initial matter, federal law tends to be woefully behind the technology. Ms. Guliani pointed out that the recent debates over GPS and cell phone surveillance technology are really debates about decades-old technologies. Location tracking and Stingray devices have been in existence for decades,²⁵ yet for decades litigants did not know which technologies were being used by police; thus, there has been no significant congressional or public discussion about these new technologies. “Right now we have a bizarre tension happening at the federal level. On one hand, we are completely unable to keep pace with the technology development. . . . When we look at some of the issues that have arisen in recent months, it really involves technology that’s almost decades old. And I am pretty certain that there are other technologies that are either in the pipeline or even being

deployed that we don't even know about yet and we haven't even had the opportunity to have a congressional or public debate about. And at the same time that we have ... this complete inability at a federal level to put in place privacy protections or civil liberties protections regarding the use of these technologies, the government is awfully good at getting these technologies out into the hands of state and local law enforcement. ... There's not really a sufficient oversight and sufficient action by the federal government to make sure that these technologies are used responsibly."

Ms. Guliani offered some suggestions to limit the expansion of these technologies, to challenge the technologies in court, and to arm the public with information to ask hard questions about the use of these technologies. She organized her suggestions around four concrete points.

End Secrecy Agreements

First, Ms. Guliani recommended a federal policy to prohibit the federal government from asking the states and localities to hide the use of new surveillance technology. As revealed through FOIA requests, the Department of Justice has encouraged local authorities to keep secret certain technologies (Stingray IMSI devices, Dirtbox DRT devices,²⁶ etc.) and thus prevent them from being litigated in court. The federal government has asked state governments to dismiss cases, hide the source of information (referring to a confidential source), or offer attractive plea deals such that defendants have no choice but to take the deal and forsake litigating the issues.²⁷ These secrecy agreements could be ended through a clear federal policy.

Inform the Judiciary about the Technology

Second, federal and state law enforcement agencies should be prohibited from withholding information about the technology from judges. In a few recent cases, judges signed warrant requests or court orders (pen trap requests) without understanding the technology at issue. Ms. Guliani discussed a case out of Tacoma, Washington, in which judges signed off on 170 orders to use cell site simulators without understanding the technology.²⁸ The orders did not explain the technology or the impact of the technology, and the judges were unaware of how the technology worked.

Require Accountability

Third, money from the federal government should not be a blank check but should be tied to standards and accountability surrounding the use of these new technologies. Accountability measures, which can be tied to funding, need to be created and enforced.

Establish Consistent Policies

Fourth, the federal government has not adopted consistent policies to cover the use of these new technologies. Because there has been little federal guidance on new technologies, states and localities have been left without rules, best practices, or guidance. Congress is doing very little in this area, and while there has been some intermittent outrage when news stories reveal use of the technology, there has not been a requirement of notification or oversight before the technologies are adopted. Congress needs to use its oversight power and be more proactive about these technologies.



Opportunities for Criminal Litigation

Hanni Fakhoury addressed some of the potential litigation opportunities that exist for lawyers in individual criminal cases. First, he recognized that we have moved to a new stage in the development of surveillance law. A few years ago, if a defense lawyer raised the issue of secret surveillance techniques, the lawyer would not have been taken seriously. Now, advocates have amassed evidence that technology like Stingray devices that capture cell phone transmissions are deployed on a systemic level across the country. Lawyers have moved beyond speculation to recognition of this fact. In Tacoma, Washington, and Baltimore, Maryland, active criminal cases have revealed that the surveillance technology has been used and has produced arrests.²⁹ In Baltimore, for example, a criminal case was dismissed because the officer testified to a “non-disclosure agreement” that prevented the officer from revealing information about the technology (presumably a Stingray device) to the court. The judge responded that there was no non-disclosure agreement with the court and the witness had to answer the question or be held in contempt. In response to the judge’s threat, the prosecution conceded the suppression motion and resolved the case. Similarly, the *Washington Post* ran a story about a Florida robbery case that was pled out to probation after the judge ordered the Stingray information disclosed to the defense.³⁰ Criminal defense lawyers can use these victories to show what is actually happening, which may lead to positive results in individual cases. In addition, the resulting media attention could result in changes to police practice. For example, in Tacoma, Washington, after a news story broke about the Stingray orders, the judges met with the police and modified the practice.³¹

New Responsibilities for Defense Lawyers

For defense lawyers, new responsibilities arise. Mr. Fakhoury suggested that if a search warrant affidavit, or a wiretap application, mentions that some source revealed a client’s information, the lawyer must ask, “Is the source a human?” “Is it a computer?” “Is it a device?” If a lawyer has a case in which the government has retained a lot of digital data (from a smartphone or a hard drive, for example), the lawyer must ask, “How long has the government held on to the data?” “What are they doing with the data?” “Are they deleting it?” Courts are starting to grapple with these issues. Lawyers can make legal arguments now when before they could not. Lawyers can use what Professor Kerr calls “the *Riley* Moment” to begin asking hard questions when digital evidence is present and to change the arguments around the collection and use of that evidence.

Why Riley Matters

As a final point, Mr. Fakhoury explained why he believed *Riley* was a significant case. First, he pointed out that the Supreme Court did not feel bound by non-digital analogies. The Court viewed digital information as different and thus found past analogies do not apply. As digital evidence expands, so will the reach of this holding. The second point is that the Court accepted that there is a quantitative and qualitative difference in cell phone data that is of constitutional significance. This insight again allows for an argument that digital information is different and, thus, lawyers and judges are not bound by prior non-digital precedent. Echoing the comments of earlier presenters, Mr. Fakhoury agreed that *Riley* signified that “data is different” in the eyes of the Supreme Court.



3. A Conversation with Joseph P. Nacchio

Joseph P. Nacchio, *Former Chairman and CEO, Qwest Communications International*

Norman L. Reimer, *Executive Director, National Association of Criminal Defense Lawyers*

Norman L. Reimer, the Executive Director of NACDL, hosted a luncheon conversation with Joseph P. Nacchio about Mr. Nacchio's experience as the CEO of a communications provider that was forced to negotiate with government intelligence officials over access to company data.

The discussion revealed a personal story of the legal consequences for those private companies and professionals who said "no" to government access to private telecommunications data. Mr. Nacchio detailed how, as former Chairman and CEO of Qwest Communications International, he had to make difficult decisions about sharing company data with government intelligence agencies. Mr. Nacchio was a highly-regarded corporate executive with close ties to government officials. He had been granted top secret security clearances and was an advisor to national security leaders. He explained how he was asked by representatives of the clandestine intelligence services to conduct covert surveillance through Qwest communication cables, and how he refused to cooperate without explicit legal authority.

Mr. Nacchio explained that as a result of his refusal, he believed he was unfairly prosecuted by the United States government. Five years after his refusal, he was indicted on insider trading charges, based on the novel claim that he had traded on the inflated stock price from secret, future government contracts. These contracts never materialized because of the company's refusal to cooperate, and thus the stock price fell. He detailed what he considered an unfair trial, with secret evidence (barred by classified information statutes [Classified Information Procedures Act]), and the inability to defend his case with information from those classified sources. The luncheon talk provided a very human example of the tensions between government access, legality, and corporate responsibility with the added twist that Mr. Nacchio was eventually convicted for having violated insider trading laws and served several years in a federal prison.

Mr. Nacchio detailed the very close relationships between the intelligence community, the defense community, and telecom companies and articulated the difficult decisions that executives in those companies had to face in determining the legality of governmental requests. Mr. Nacchio's former company Qwest Communications International was the only company to refuse to provide information to the government, and he believes that as a result the company lost over \$500 million in government contracts.

Mr. Nacchio also detailed the difficulties of being prosecuted by the Department of Justice, the challenges of prison, and the consequences of being a convicted felon. Specifically, he detailed the unique position of being an unindicted target of a criminal investigation with a defense based on classified information, but without lawyers who had been granted the appropriate clearances. He detailed the surreal experience of trying a criminal case where defenses, evidence, and witnesses were precluded based on secrecy grounds, and the distorting effect of CIPA on the truth-finding procedures of trial. The resulting case was decided by a jury that was precluded from hearing all of the evidence, including his main defense argument.

Mr. Nacchio also detailed the difficulty of a white collar defendant being sent to a federal prison, the seven weeks of travel by the US Marshals, solitary confinement, and poor living conditions. He also recounted the warm feelings he felt toward the fellow prisoners he met in federal prison, and the incredibly difficult challenges for all returning citizens with felony records.



Mr. Nacchio concluded his talk by reminding the audience that freedom — and the privilege of freedom — was the most important lesson he learned from his experience. He warned the audience that they are giving up their freedom based on claims of national security and encouraged the audience to continue to fight for that privilege of freedom.

4. Law and Policy: A Path Forward for the Constitution, Courts, Congress, and Law Enforcement

MODERATOR:

Jeff Rosen, *President and CEO, National Constitution Center;*
Professor of Law, George Washington University Law School

DISCUSSANTS:

Ahmed Ghappour, *Visiting Professor, UC Hastings College of the Law;*
Director, Liberty, Security and Technology Clinic

David Lieber, *Senior Privacy Policy Counsel, Google*

Greg Nojeim, *Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy and Technology*

Kenneth Wainstein, *Partner, Cadwalader, Wickersham & Taft LLP;*
Former Homeland Security Advisor; Former Assistant Attorney General for National Security, DOJ; Former United States Attorney for the District of Columbia

Jeff Rosen introduced the third panel as a look to the future of the Fourth Amendment in the digital age and possible congressional changes to surveillance laws in the coming years.

The Mini-Drone Hypothetical

Professor Rosen framed the panel discussion with a hypothetical question he asked each of the panelists to answer. Professor Rosen posited: “Imagine that tomorrow, President Obama said that in order to protect the security of America, tiny drones would be sent flying in the air with minuscule cameras attached. Using these drones, the government would reserve the right to focus on anyone, say me, follow me to see where I was going. If the images were archived, they could go back and follow me backward to see where I came from and basically allow 24/7 ubiquitous surveillance of any person in the world. The question I want to ask the panel to engage in is — would this violate the Fourth Amendment to the Constitution?”

No Constitutional Violation, but It Depends

Professor Ahmed Ghappour responded by recognizing the answer might be contextual: “Like any good attorney, I will say it depends.” He explained that the answer might depend on how big the drones are, or how close they get to the targets. Also, an open question would be whether the data from the drones are aggregated or processed. Depending on the answers to these questions, the Fourth Amendment analysis might change. Professor Ghappour emphasized the real difference between collection and use from a doctrinal perspective. Currently, there are few limitations on collection of public information in public spaces. Professor Ghappour also pointed out that such a hypothetical was not so futuristic and public space surveillance is quite common. As he explained, we have technologies that allow for license plates to be monitored and cameras all over the city. From one perspective, because all of this is public information, one might not have a reasonable expectation of privacy when walking around on a public street. To answer the question, Professor Ghappour concluded, the current doctrine would probably allow mini-drone surveillance in public space under the Fourth Amendment.

The technologies that actually conduct the analytics are increasingly sophisticated. You have technology that implements artificial technology and learning and so the goal for a lot of this big data stuff is that the algorithm can identify patterns that humans are not cognitively capable of doing on their own. And so you got a situation where a computer is telling you that this person is a bad person and you should follow them, or you should search them, or you should arrest them, or possibly drone them — at an accuracy that is higher than any human analyst, but you don't know why. I think that's sort of the question for us. When you have a very highly reliable algorithm that cannot articulate why it's giving you an outcome and that outcome is one of culpability, what do we do?

Ahmed Ghappour



Professor Ghappour highlighted a few other issues that might arise beyond the question of data collection. While collection in the public sphere is important, so is what happens to the data once collected. All of the new technologies discussed will result in the government having more and more data to analyze. “The technologies that actually conduct the analytics are increasingly sophisticated. You have technology that implements artificial technology and learning and so the goal for a lot of this big data stuff is that the algorithm can identify patterns that humans are not cognitively capable of doing on their own. And so you got a situation where a computer is telling you that this person is a bad person and you should follow them, or you should search them, or you should arrest them, or possibly drone them — at an accuracy that is higher than any human analyst, but you don't know why. I think that's sort of the question for us. When you have a very highly reliable algorithm that cannot articulate why it's giving you an outcome and that outcome is one of culpability, what do we do?” At the point when the big data computer is producing tips of suspicious behavior based on highly reliable algorithms, the question is what should be done with this information. We might know the algorithm is accurate, yet not know why it is accurate and be unable to investigate the reasons behind the data-driven tips.

Constitutional Violation under Katz

David Lieber also began by answering the hypothetical with an eye toward current Fourth Amendment doctrine. Mr. Lieber concluded that fundamental Fourth Amendment principles post-*Katz*, focusing on people not places, lead him to conclude that such ubiquitous and suspicionless mini-drone monitoring 24/7 of a person would violate the Fourth Amendment.

A Legislative Response

Mr. Lieber went on to discuss some of the other pressure points arising from the discussion of new technologies like those in the hypothetical. He stated there was reason to be sanguine about the development of case law, but that issues of “standing” may thwart potential legal challenges to such surveillance. Because the technologies remain secret, and even unacknowledged by law enforcement, it



may be difficult to demonstrate concrete harm from their use. Fourth Amendment standing — the cases and controversies requirement — will likely prevent a lot of cases from ever being resolved by the courts. As such, he expressed more confidence in a legislative fix to some of the problems.

Mr. Lieber detailed a rather optimistic view of Congress's ability to address new technological challenges to surveillance. He pointed to two areas of progress. First, he expressed optimism that Congress would amend the 1986 Electronic Communications and Privacy Act (ECPA).³² As part of the Digital Due Process coalition,³³ Google and other companies have been working to update the Act to codify a warrant requirement to obtain the content of communications data. This update would, he suggested, comport with many users' reasonable expectation of privacy. For example, at the heart of ECPA is the "180 rule" which mandates a warrant for the content of stored emails within 180 days, but no warrant after that time period. Thus, on the 181st day, all of the content of one's stored email communications can be subpoenaed. While the Sixth Circuit Court of Appeals has required such a warrant, and many service providers also require a warrant as a matter of practice, the federal law remains outdated. Mr. Lieber explained that the current ECPA reform bill has 312 co-sponsors in the House of Representatives and would likely pass both the House and the Senate.

Second, Mr. Lieber discussed the renewal of Section 215 of the USA Patriot Act, which expires in May 2015. He reminded the audience that the debate has largely centered around FISA and how or whether it should be modified. Mr. Lieber concurred with others who recommended that the Section 215 program be reformed, citing both issues of effectiveness and legality. Mr. Lieber discussed some of the debates around Section 215 and other provisions that impact collection of communications and bulk metadata.

Finally, Mr. Lieber flagged the growing issue of objects in "the Internet of Things" and the fact that new legislative rules may be needed to address this technology. Currently, many open questions exist about whether ECPA or any other statute covers electronic communications within the Internet of Things. These smart objects linked by sensors and connected through the Internet might include data from a home Nest Learning Thermostat, which can turn off the lights when a homeowner leaves for the day or turn them on before the homeowner enters the house, to other monitors (e.g., Dropcam surveillance videos³⁴) that can record and send information about a person's daily patterns of behavior. These devices provide a lot of detail about daily habits and ought to be the subject of statutory protection. However, because ECPA has remained unchanged since 1986, the law may not cover these new innovations. He raised this issue as one of many growing questions that will arise from the growth of remote computing services.

Constitutional Violation under Jones

Responding to the hypothetical, Mr. Nojeim remarked that the Supreme Court had been asked to consider a similar issue in *United States v. Jones*, and had rejected the argument that just because individuals are in public they have no Fourth Amendment protection. Mr. Nojeim explained that while the *Jones* case was decided on trespass grounds, the government had argued to the Supreme Court that being in public should mean that individuals had given up their right to privacy. However, none of the justices in *Jones* agreed with that argument, and so he believed the Supreme Court would find the mini-drone surveillance unconstitutional.

A Pessimistic Vision of the Digital Fourth Amendment

Mr. Nojeim framed his remarks by offering three reasons to be pessimistic about the Fourth Amendment in the digital age and three reasons to be optimistic.

As to the concerns, Mr. Nojeim highlighted three Fourth Amendment doctrines that are indirectly weakening the protection of citizens in a digital surveillance world. First, he explained that the “administrative search doctrine”³⁵ has been expanded because of enhanced technologies. As one example, airport screenings have become much more invasive: What used to involve a relatively non-intrusive metal detector search (magnetometer search) has now become an electronic strip search that reveals information about what is happening underneath our clothing. Second, the FISA court that deals with national security issues has issued an opinion that creates a national security exception to the Fourth Amendment.³⁶ Such a blanket exception offers a tremendous loophole for privacy protections. Third, the digital footprints we create are being collected by third parties, and the Supreme Court’s third-party doctrine³⁷ denies those footprints Fourth Amendment protection. Without reform to the third-party doctrine, many consumer services will eventually become surveillance resources for the government.

The last thing I want to mention that gives me hope is encryption. The idea that people can encrypt their data to make it so that the bad guys can’t get it and if they do get it, they can’t really use it well; the strong protection that encryption can provide and the increasing ease with which we can encrypt our data.

Greg Nojeim

An Optimistic Vision of the Digital Fourth Amendment

On the positive side, Mr. Nojeim articulated three reasons to be optimistic about a digital Fourth Amendment. First, he pointed to the Supreme Court’s growing embrace of the notion that technology poses real threats to privacy that cannot be resolved by merely looking at the non-technological analogue. This “technology is different”/ “data is different” rationale can be seen in the *Kyllo* case in 2001 where the Supreme Court ruled that the use of thermal imaging to explore activity in a private home requires a warrant. It can also be seen in *Jones* where the Court ruled that tracking a car for 28 days by attaching a GPS device required a warrant. And, most recently, in *Riley v. California*, the Supreme Court ruled that police cannot search a cell phone possessed by an arrestee without a warrant. In *Riley*, the government had argued that if police had found something non-digital in Riley’s pocket they would be entitled to search the item, so, by extension, they should be able to search the cell phone. The Court rejected the argument, holding that cell phones are different because they carry so much data and thus need a greater level of protection.

A second positive signal is that business has taken on privacy issues in a way that is unprecedented. Companies like Google and other tech giants have realized that privacy is good for the bottom line. This has improved consumer trust, and has come to be seen as essential for technology companies to sell their products. As a result, business has become a powerful new constituency in the debates in Congress. Even more positive, many of these companies are also litigating privacy issues in court. Companies like Yahoo have been defending data privacy interests against the government in large and costly lawsuits. With industry lawyers and lobbyists in support, privacy advocates will have an easier time arguing for more protective laws.

Finally, Mr. Nojeim expressed optimism that encryption might fundamentally alter the Fourth Amendment analysis. The third-party doctrine becomes unavailing if the third-party cannot, itself, unlock the data. “And



the last thing I want to mention that gives me hope is encryption. The idea that people can encrypt their data to make it so that the bad guys can't get it and if they do get it, they can't really use it well; the strong protection that encryption can provide and the increasing ease with which we can encrypt our data."

This is an ongoing issue. Technology evolves, the Fourth Amendment was drafted a couple hundred years ago or more and it has to adapt to this new technology. . . . There is a healthy debate about that and that results in the FISA Amendments Act that allowed the 702 collection that we were talking about; geo-location technology and the *Jones* decision and now encryption. So we have these issues that have come up — and this is a perennial issue — the courts have to deal with them as a constitutional matter of interpretation of existing law. The public has to deal with them in this kind of context and really think about how we want to balance security vs. privacy. I shouldn't say vs. privacy because I don't think they are necessarily adversarial but security and privacy. And then, most importantly, Congress actually has to decide where to draw those lines inside the constitutional lines that determine where the government can go and under what conditions in terms of surveillance.

Kenneth Wainstein

A Slippery Slope

In response to the hypothetical, Mr. Wainstein cautioned that the questions about drone surveillance are not so simply answered. He clarified that the *Jones* decision turned on a narrow trespass rationale and, thus, the lines about when 24/7 surveillance become a search remain largely unanswered. While one might acknowledge that 24/7 high-detail, mini-drone surveillance feels intrusive, it might be hard to distinguish this technology from some other equally invasive surveillance technologies. Further, it might be difficult to distinguish drones from non-technological surveillance that is equally intrusive. The standard of a reasonable expectation of privacy does not easily address these slippery slope arguments. For example, he queried, how do we distinguish 24/7 human police surveillance for terrorist suspects that is done every day of the year? Do police need to get a warrant for this now, even if all of the observation takes place in public? Mr. Wainstein argued that society wants the terrorist suspect watched, and these types of surveillance are necessary on occasion. Or, he asked, what about CCTV feeds that provide equivalent surveillance coverage in public, but currently do not require a warrant. The difficulty again is the slippery slope, and unless that argument can be addressed, Mr. Wainstein did not see the Supreme Court going down that path toward expanding *Jones*.

Technological Change in Context

Mr. Wainstein also addressed some of the policy issues that Congress and the courts will confront in the next few years. He stated that technological change is a constant. Technological change created the *Katz*³⁸ decision

with the introduction of payphones. Technological change created the *Smith v. Maryland*³⁹ decision with bulk collection of phone records. The FISA statute was passed in 1978 before there was such thing as email, and many of the assumptions in the original law have since been turned on their heads because of technological changes; but this is to be expected. “This is an ongoing issue. Technology evolves, the Fourth Amendment was drafted a couple hundred years ago or more and it has to adapt to this new technology. . . . There is a healthy debate about that and that results in the FISA Amendments Act that allowed the 702 collection that we were talking about; geo-location technology and the *Jones* decision and now encryption. So we have these issues that have come up — and this is a perennial issue — the courts have to deal with them as a constitutional matter of interpretation of existing law. The public has to deal with them in this kind of context and really think about how we want to balance security vs. privacy. I shouldn’t say vs privacy because I don’t think they are necessarily adversarial but security and privacy. And then, most importantly, Congress actually has to decide where to draw those lines inside the constitutional lines that determine where the government can go and under what conditions in terms of surveillance.” At its core, the old debate between security and privacy must be considered not as adversarial interests, but interests that need to be balanced (and re-balanced). Congress must again attempt to draw the lines to determine what the government can do and what the conditions on surveillance should be consistent with that balance.

Going Dark

Mr. Wainstein applauded the legal and legislative debate, and raised the related issue of encryption and law enforcement’s concern with “going dark.” The debate over going dark is the debate over encryption technology that makes it impossible for third-party service providers or anyone else to access smartphones and other devices. Law enforcement is quite concerned about this lack of access to encrypted data in the devices. Mr. Wainstein also echoed a concern that national security and law enforcement interests might suffer with such significant access limitations.

It’s politically difficult for Congress to do that (curtail the governments surveillance capabilities). . . . When you’re talking about national security authorities, if the government can come and the executive branch can come in and make a strong argument for the authority, the power that they have been given in that authority, and why they should maintain it and give examples of how it has been useful, it’s politically difficult for Congress to really scale back and deny them that authority.

Kenneth Wainstein

Mr. Wainstein also raised the question whether there might be a dramatic curtailment by Congress of the government’s foreign surveillance capabilities in the national security context. Mr. Wainstein thought this second concern not likely because of the political reality surrounding the repeal or weakening of government surveillance techniques. “It’s politically difficult for Congress to do that (curtail the government’s surveillance capabilities). . . . When you’re talking about national security authorities, if the government can come and the executive branch can come in and make a strong argument for the authority, the power that they have been given in that authority, and why they should maintain it and give examples of how it has been useful, it’s politically difficult for Congress to really scale back and deny them that authority.” With new



threats like ISIS and other concerns in the aftermath of the Arab Spring, Mr. Wainstein thought that there would be no denial of authority and only a limited increase in restrictions on current surveillance capabilities.

Three to One, Mini-Drones Are Unconstitutional

Professor Rosen summarized the vote on his drone hypothetical as three votes finding the 24/7 surveillance by a mini-drone a violation of the Fourth Amendment and one vote finding no violation. Professor Ghappour responded in dissent that the issue is really the aggregation problem not the 24/7 collection problem, and the aggregation would also have a chilling effect on First Amendment freedoms. The focus should be on use — how the aggregated information might be used by the government. Mr. Nojeim countered that persistence will be key. Mr. Nojeim defined persistence as the problem of continuing surveillance, which he argued would itself be enough under the Fourth Amendment to find a violation of an expectation of privacy.

Private Surveillance: The Open Planet Problem

Professor Rosen asked the panelists to consider a new hypothetical: What would happen if a large information technology company such as Facebook created a new “app” called “Open Planet” to collect all of the current surveillance camera feeds in the world and to broadcast it live on Facebook? Assume the company also encouraged people to broadcast live from their phones, so that anyone could follow anyone else with an iPhone and broadcast that image 24/7 on the Internet. While obviously the Fourth Amendment does not apply, because the company is not a governmental actor, these types of companies arguably have more power over privacy and free speech than any other actor in the political system. So, Professor Rosen asked, could Facebook or its equivalent broadcast its own private 24/7 camera feed that would allow 24/7 tracking of anyone in the world?

This is what Europeans refer to as data protection, which I distinguish from privacy. In my own line of thinking, I think there is a difference between invading someone's expectation of privacy, in our case collecting data. I think there is a difference between that and then using the data for a variety of purposes and whether the user, the one that gave you the data, actually has control over that.

Ahmed Ghappour

Private Companies Need Privacy Protocols

David Lieber answered that he felt confident that any private company that undertook such a project would have specific privacy protocols behind it. So, if such a product existed, there would be robust controls around the collection and use of that information, and likely legal restrictions on the ability of a company to collect and use that information. While this is more a question of privacy protocols than issues of government surveillance discussed earlier, there could be an intersection of statutory law with the new product. For example, ECPA protections might be violated if the collected information were shared with a third-party without the original user's consent to that type of disclosure. According to Mr. Lieber, the key in any new privacy challenge is to give users control of their own information.

Open Planet Would Exist Largely Unregulated

Mr. Wainstein commented that he did not see any clearly applicable statutory bar for such a private (non-governmental) program like Open Planet. While not supportive of the idea, he saw no statutory or constitutional barrier to such a program.

Mr. Nojeim concurred that under existing statutory law nothing prevented this type of private collection of public information. Nor did Mr. Nojeim believe any of the proposed statutory amendments currently being considered by Congress would cover this type of private collection.

Data Protection v. Privacy

Mr. Nojeim suggested that another concern with Open Planet might be that the information would be of interest to the government. Even if privately collected, the government could seek to obtain it, either through law enforcement requests or simply purchasing the information like any other consumer. Mr. Nojeim commented that privacy cannot simply be thought of as preventing collection, but also must consider how to protect that data from government use if such protections are deemed necessary.

Professor Ghappour noted that “[t]his is what Europeans refer to as data protection, which I distinguish from privacy. In my own line of thinking, I think there is a difference between invading someone’s expectation of privacy, in our case collecting data. I think there is a difference between that and then using the data for a variety of purposes and whether the user, the one that gave you the data, actually has control over that.” Thus, even if individuals have given up information such that they no longer have privacy in the data, they might still have an argument to control use of that data. The fact that someone provided the information to a third-party should not mean that they lose control of that information vis-a-vis all parties.

The Right to Be Forgotten

Mr. Lieber mentioned the debate in Europe over “the right to be forgotten”⁴⁰ and the legal challenge Google lost in the European Court of Justice over the issue. Google is currently trying to implement the decision, meaning deleting links that run afoul of the ruling. As a consequence of the decision, Google and other large companies are responsible for controlling what information is available on the Internet. Mr. Lieber expressed discomfort that any company would have the ability to control information and essentially excise information from the public domain. He argued that this ruling has an impact on democratic and associational values, especially in the United States with its unique and valuable First Amendment protections.

The discussion continued about the right to be forgotten and the difficult position companies like Google are in to determine whether someone who requests that a link be deleted falls within a category of public figure or whether the information is otherwise relevant. As was discussed, if Google should guess wrong about the appropriateness of deleting information about a person who wishes to be forgotten on the Internet, the company is liable for civil fines.

Mr. Wainstein agreed that such a project would be difficult to implement and administer. Further, such a project would seemingly undermine democratic values that underlie freedom of expression and the marketplace of ideas, which is nourished by more information as opposed to less information.



Third-Party Doctrine Challenges

Professor Rosen then asked about the legislative proposals pending in Congress concerning the third-party doctrine.

Mr. Nojeim responded that the proposed ECPA amendments would require a warrant to obtain the content of communications. In addition, there is the Geolocation Privacy and Surveillance Act (GPS) Act⁴¹ which would require the government to get a warrant for information generated by the use of mobile devices like cellphones. The GPS Act is not as far along in the process and might face more debate. One problem that would need to be addressed is cell tower dumps, whereby police are able to vacuum up all of the cell phone numbers at a given location at a given time. The question is whether police need a warrant to obtain this information, or whether they need some other information to isolate the numbers requested. These are difficult issues that remain unresolved. In addition, the debate over Section 215 surveillance will continue this spring. Congress is facing an important decision about whether to continue to permit bulk collection of information about virtually every phone call made to, from, or within the United States. Finally, there is cybersecurity legislation pending right now that would allow companies to share what they call cyber threat indicators that are derived from communications with the government, not just for cybersecurity reasons but also for criminal reasons. The question is whether statutory law will trigger voluntary disclosure of information from providers to the government. Mr. Nojeim expressed some concern at the broad language of current proposals that would go beyond voluntary disclosures.

Future Debates

Finally, Professor Rosen asked the panel to consider three major issues that will be considered in Congress in the next year: (1) bulk collection as part of Section 702 of the FISA Amendments Act; (2) a warrant requirement for content and geolocation information; and (3) cybersecurity.

Bulk Collection

Professor Ghappour expressed his opinion that a statutory ban on bulk collection is necessary because the Fourth Amendment may not cover the issue.

Mr. Wainstein argued that such a ban might harm law enforcement, but that important questions of constitutionality and utility do need to be addressed. The question is whether government access can be ensured but with appropriate safeguards. Sometimes the practical realities require access to bulk collection, even though the collection technologies are overbroad. For example, Mr. Wainstein hypothesized a tip that a particular terrorist is boarding a particular plane. Unless all of the passenger lists of all of the airlines are collected, police could not identify that particular list in time to prevent the terrorist act. The bulk collection of passenger lists — which obviously includes all names, not just the terrorist's — is necessary to identify the terrorist in time. The important point is not the collection, but the targeted use. As long as the use is targeted, the bulk collection is justified.

Mr. Nojeim modified the discussion by calling the collection of particularized lists of information “bulkish collection,” whereby information is collected but without an identifier to collect on a specific term. The issue, he said, is what happens to those people who do not match the target. What happens to people whose names were bulk collected on the airline passenger list but not flagged as a terrorist? Should that information be destroyed, deleted, or forgotten? Currently, the FBI has no protocols on the retention of this bulk information. Resolving this question of what to do with the data is an important one for the future.

Mr. Lieber expressed his support for the USA Freedom Act, which would cover some of these bulk collection limitations. He suggested that Congress has developed a promising solution that has buy-in from industry, government, and privacy advocates. This bill, he believed, has enough safeguards and should be passed into law.

Content/Geolocation Data

Next, the panelists discussed whether legislation requiring a warrant to obtain content or geolocation data would be passed by Congress. Mr. Wainstein suggested that some parts of ECPA — namely the 180-day rule to obtain content with a warrant — may pass with bipartisan support. Mr. Nojeim expressed his skepticism about Congress passing a strong bill protecting geolocation or content, but felt confident that ECPA reform will pass. Already most providers require warrants for content, even though the statutes at issue do not explicitly require it.

Encryption

Finally, the panel discussed the issue of cybersecurity and the move by companies to provide encrypted technologies that prevent law enforcement from gaining access to private data stored on a device. Professor Ghappour conceded that encryption would have a negative effect on law enforcement investigation, but argued that companies should be able to provide the most secure and robust technology available. Any security backdoors that would allow law enforcement access would also allow access to hackers who would undermine the security of the device. The fact that encryption might have a negative impact to law enforcement does not outweigh the positive benefits to consumers.

Mr. Lieber stated that Google was moving toward a more encrypted stance similar to Apple's decision to encrypt its smartphones. Google has been working on end-to-end encryption for many years, and Google has been looking at things from a security angle. Identity theft is one of the real dangers of the modern world, and so security more than surveillance has been driving the move toward encryption. In terms of the cybersecurity bill, Google has not taken a position on it, but there are real process questions about taking up a bill that impacts privacy before taking up a bill that focuses on government surveillance.

Mr. Wainstein expressed his concern that the move toward complete encryption will negatively impact law enforcement and make it more difficult to thwart terrorism. Mr. Wainstein proposed a robust warrant requirement that would strike a fair balance between technology security and law enforcement need, allowing some access to otherwise encrypted data.



Summary and Recommendations

The symposium provided a wide-ranging discussion on how the Fourth Amendment might change in a digital world and how defense lawyers might adapt to this change. Throughout the day, participants suggested several specific recommendations. While no formal recommendations were adopted or agreed to, several common themes emerged to provide a focus for future engagement. These recommendations targeted four areas of change: (1) legal strategy; (2) education; (3) legislative advocacy; and (4) policy.

Legal Strategy

Defense lawyers play a key role in shaping the legal response to new technological developments. From developing a shared litigation strategy, to identifying Fourth Amendment issues, to challenging new surveillance techniques, lawyers must play a leading role in this change. Specific recommendations included the following:

- 🔗 Litigators should develop Fourth Amendment suppression strategies focused on new Supreme Court cases such as *United States v. Jones* and *Riley v. California*. In both *Jones* and *Riley*, the Supreme Court appeared willing to look anew at challenges to digital surveillance of personal information.
- 🔗 Lawyers should litigate based on the newly rediscovered Fourth Amendment “trespass theory” that arises from Justice Scalia’s opinion in *United States v. Jones*.
- 🔗 Litigators should challenge all long-term and aggregated surveillance techniques, arguing that such collection of information is equivalent to a “mosaic theory search” recognized by the five concurring justices in *United States v. Jones*.
- 🔗 Defense counsel should look for what Professor Kerr called “*Riley* Moments” in which older, pre-digital precedent no longer applies to the digital capture of information. Defense lawyers should use *Riley* to suggest that cases involving digital evidence should be treated differently than cases involving non-digital evidence. This “data is different” argument should be emphasized in litigation and public education.
- 🔗 Lawyers, as a group, should develop shared litigation strategies to challenge surveillance practices at the national and local level. Specifically, lawyers should share materials on how to litigate and challenge new technologies such as Stingray devices (or equivalent IMSI capture technologies).
- 🔗 Litigators should challenge the scope of authority for domestic surveillance. The blurring of foreign surveillance into domestic law enforcement must be policed.
- 🔗 Defense lawyers have a new obligation to seek discovery about the source of law enforcement information to determine if the prosecution has exploited new (and sometimes secret) surveillance technologies.
- 🔗 Lawyers must develop a sustained challenge to the existing “third-party doctrine,” which removes significant Fourth Amendment protections of personal data. Organizations, bar associations, and academics must seek to reconceive how personal data is considered for Fourth Amendment purposes.

Education

The symposium panelists emphasized that any response to new technological threats must be addressed by educating the public about the impact of these new surveillance challenges. In addition to educating the public, lawyers must also educate judges and other lawyers about the existing surveillance dangers. This three-pronged educational approach will begin the process of developing an awareness of a largely secret problem.

Three specific recommendations emerged from the panels:

- 🎧 A national campaign to educate the public about the growth of the surveillance state needs to be articulated and funded. As one panelist stated, “Too much has been going on in secret for too long.” Citizens have not been engaged in the debate because most of the developments have been hidden. This project should promote the ideas of technologists, legal scholars, and institutions that have identified constitutional threats to privacy and liberty. More public notice and public debate will counter the trend to accept secrecy as a cost of security.
- 🎧 A parallel educational project needs to be developed to educate judges about how to think about new technology. Many judges are not technologically sophisticated about cutting edge surveillance techniques. An education program should include programs for judges to learn about existing technologies. This program should continue the progress of this symposium by linking Fourth Amendment scholars, technologists, and policy experts to discuss how the courts should respond to these changes.
- 🎧 Lawyers need to educate themselves about the technology underlying these new surveillance techniques. Lawyers, like judges, tend not to be technologists but must begin learning the basics of how network operations and network security works. In addition, lawyers must be sufficiently conversant with these techniques to effectively litigate the issues in court. Bar groups should begin lawyer-focused education programs to engage colleagues in re-examining the source and authority of government intelligence.

Legislative Advocacy

Underlying much of the symposium’s discussion was a recognition that the legislative landscape remained far behind the technology. Panelists recognized the need to change the laws to reflect new surveillance techniques, new technologies, and new law enforcement practices, but also acknowledged that the current legislative environment made such change difficult. While panelists discussed some specific legislative proposals, three more general recommendations appeared to gain consensus.

- 🎧 The defense bar should play a key role in shaping legislative changes by providing stories about how new digital searches and technological surveillance are being implemented on the ground. Many of the proposed laws have been shaped by criminal cases or news stories. Discussion about foreign intelligence collection arose from the Edward Snowden revelations. Discussion about geo-location legislation arose after *United States v. Jones*. Discussion of cell-tower surveillance arose from federal court litigation.



- ☞ The technology companies involved in developing and maintaining the new digital age have been on the side of privacy advocates when it comes to advocating for protections in new legislation. Attorneys should encourage partnerships with business interests who might be able to create technological solutions and also have the financial resources and political capital to influence legislation.
- ☞ Consider both state and federal legislative remedies. State legislatures and even local legislatures have acted to curb surveillance techniques, so the focus should not be limited to merely congressional action.

Policy

The symposium also generated specific policy recommendations to alter what was seen as the largely unregulated governmental use of new surveillance technologies. These policy proposals are steps that the federal government (or local governments) could take before adopting any new technologies and to improve existing oversight.

- ☞ End federal secrecy agreements. Federal policy should prohibit federal agencies from demanding that states and localities hide the use of new surveillance technology. In some cases, in order to receive the new digital surveillance tools, a secrecy agreement must be signed. These agreements are unnecessary and undermine transparency.
- ☞ Require standards and accountability to the federal government by local governments in order to use new technologies financed by the federal government. Currently, the technologies are provided without accountability mechanisms to ensure they are used as intended.
- ☞ Require the federal government to adopt consistent policies to cover the use of new technologies. Currently, many technologies (for example the Stingray device) are provided without any standard operating policies.
- ☞ Promote technological solutions like encryption. While encryption is a contested topic — pitting technologists interested in data security against law enforcement interested in data access — it also provides a solution to government surveillance. The idea that people can encrypt their data to make sure that “bad guys” and others (including the government) cannot get the information provides some hope for a technological fix for otherwise large-scale surveillance. As encryption becomes easier to use, the hope is that protections of personal data will increase. Thus, even if the law (or courts) cannot catch up with data security, the technology might offer a solution
- ☞ Refocus the problem of privacy as one of data protection. A data protection focus asks what individuals can do to control the data already collected, whereas a privacy focus asks how data is being collected. This distinction is central to the surveillance debate in Europe and might be helpful to the ongoing discussions in America.
- ☞ Require notice of the origin of the evidence in all criminal cases. Defendants should have the right to know from what program or technology the evidence being used against them was derived.

1. Andrew Guthrie Ferguson is a Professor of Law at the University of the District of Columbia. Professor Ferguson teaches and writes in the area of criminal law, criminal procedure, and evidence. He is a national expert on juries, predictive policing, and the Fourth Amendment. See <http://www.law.udc.edu/?AFerguson>.

2. *Riley v. California*, 134 S. Ct. 2473 (2014).

3. *United States v. Jones*, 132 S. Ct. 945 (2012).

4. 134 S. Ct. 2473 (2014).

5. Bill Snyder, *Snowden: The NSA Planted Backdoors in Cisco Products*, INFOWORLD (May 15, 2014), available at <http://www.infoworld.com/article/2608141/internet-privacy/snowden—the-nsa-planted-backdoors-in-cisco-products.html>.

6. FINAL REPORT OF THE SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK 1, S. Rep. No. 755, 94th Cong., 2d Sess. 71, 128 (1976).

7. Two major developments occurred after the symposium regarding the implementation of Section 215 of the Patriot Act. First, on May 7, 2015, a three-judge panel of the U.S. Court of Appeals for the Second Circuit issued a long-awaited decision in *American Civil Liberties Union v. Clapper*, finding that the government's broad interpretation of Section 215 of the Patriot Act could not be squared with the plain language of the statute and finding the government's bulk meta data collection program illegal. See generally *American Civil Liberties Union, et al. v. Clapper, et al.*, No. 14-42 (2d Cir. (2015)). A few weeks later, Congress passed the USA Freedom Act, which reined in the government's bulk collection of phone records and other records under Section 215 of the Patriot Act. (USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268, available at <https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf>).

8. 50 U.S.C. § 1861(a)(1).

9. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2441 (to be codified at 50 U.S.C. § 1881a(h)(3)).

10. Protect America Act of 2007, Pub. L. No. 110–55, 121 Stat. 553, 50 USC 1801, available at <https://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm>.

11. FISA Amendments Act of 2008, Pub. L. No. 110-261, available at <https://www.govtrack.us/congress/bills/110/hr6304/text>.

12. Exec. Order No. 12333, 46 FR 59941.

13. Ewen MacAskill, *Yahoo Files Lawsuit Against NSA Over User Requests*, THE GUARDIAN (Sept. 9, 2013), available at <http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests>; Charles Arthur & Dominic Rushe, *NSA Scandal: Microsoft and Twitter Join Calls to Disclose Data Requests*, THE GUARDIAN (June 12, 2013), available at <http://www.theguardian.com/world/2013/jun/12/microsoft-twitter-rivals-nsa-requests>.

14. Adi Robertson, *Microsoft Moves Forward With NSA Surveillance Lawsuit After Government Negotiations Stall*, VERGE (Aug. 30, 2013, 2:29 PM), available at <http://www.theverge.com/2013/8/30/4676538/microsoft-moves-forward-with-nsa-surveillance-lawsuit/in/4167369>.

15. Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 137 (2014).

16. See, e.g., Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1288 (2014).



17. See generally *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980); *United States v. Brown*, 484 F.2d 418, (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974); and *United States v. Buck*, 548 F.2d 871 (9th Cir. 1977).

18. See, e.g., Stephen E. Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and Its States Analogs to Protect Third-Party Information From Unreasonable Search*, 55 CATH. U. L. REV. 373, 378 (2006); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007).

19. See note 14.

20. 134 S. Ct. 2473 (2014).

21. *Davis v. United States*, 131 S. Ct. 2419 (2011).

22. 132 S. Ct. 945 (2012).

23. *Grady v. North Carolina*, 575 U.S. ____ (2015).

24. *Kyllo v. United States*, 533 U.S. 27 (2001).

25. "The first IMSI Catchers date back as early as 1993 and were big, heavy, and expensive. Only a few manufacturers existed and the economic barrier limited the device's use mostly to governmental agencies. However, in recent years, a number of smaller and cheaper as well as self-built projects appeared making cellular network snooping attacks feasible to much larger audiences." Adrian Dabrowski et al., *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers*, available at <https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf> (internal citations omitted).

26. "The planes carry 'dirtboxes,' known as such due to the initials of the unit of Boeing that manufactures them, namely Digital Receiver Technology. These devices are capable of mimicking the cell towers of telecommunications companies, tricking mobile phones into reporting the unique registration data that each device holds. The devices only measure two feet, but they are capable of retrieving information from tens of thousands of mobile phones during a single flight. The information allows investigators to obtain the identifying information of the mobile phones, along with the general location of their users." Aaron Mamiit, *U.S. Using Planes Equipped With 'Dirtbox' to Spy on Your Phone Calls*, TECH TIMES, November 16, available at <http://www.techtimes.com/articles/20282/20141116/us-using-dirtbox-equipped-planes-to-spy-on-your-phone-calls.htm>.

27. Neema Singh Guliani, *How Does Someone Get 6 Months' Probation for a Crime Carrying a 4-Year Minimum Sentence?*, April 2, 2015, available at <https://www.aclu.org/blog/how-does-someone-get-6-months-probation-crime-carrying-4-year-minimum-sentence>.

28. Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, The News Tribune (November 15, 2014) available at <http://www.thenewstribune.com/news/local/crime/article25894096.html>.

29. Justin Fenton, *Guilty Pleas in Case Involving Controversial Tracking Device*, BALTIMORE SUN (January 7, 2015), available at <http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-plea-deal-20150107-story.html>.

30. Ellen Nakishima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASHINGTON POST (February 22, 2015), available at https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

31. See note 28.

32. 18 U.S.C. § 2518 (1986).

33. NACDL is a member of the Digital Due Process coalition.

34. Dropcams are surveillance cameras that can be purchased for a modest amount of money and placed in homes to monitor activity. Images are streamed to a computer or cellphone and video is backed up by cloud storage. *Dropcam Pro: A Baby Monitor or a Security System?*, Security Gem (January 17, 2015), available at <http://www.securitygem.com/dropcam-pro-a-baby-monitor-or-a-security-system/>.



35. See, e.g., Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255 (2011).


36. See, e.g., L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343, 1345 (2013).

37. See note 18.

38. *Katz v. United States*, 389 U.S. 347 (1967).

39. *Smith v. Maryland*, 442 U.S. 735 (1979).

40. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 91 (2012).

41. Geolocation Privacy and Surveillance Act of 2015, S. 237, 114th Congress (1st session 2015) available at <https://www.congress.gov/114/bills/s237/BILLS-114s237is.pdf>. 



Appendix A — Biographies

Catherine Crump is an Assistant Clinical Professor of Law at UC Berkeley School of Law and Associate Director of the Samuelson Law, Technology & Public Policy Clinic. An experienced litigator specializing in constitutional matters, she has represented a broad range of clients seeking to vindicate their First and Fourth Amendment rights. She also has extensive experience litigating to compel the disclosure of government records under the Freedom of Information Act.

Professor Crump's primary interest is the impact of new technologies on civil liberties. Representative matters include serving as counsel in the ACLU's challenge to the National Security Agency's mass collection of Americans' call records; representing artists, media outlets and others challenging a federal internet censorship law; and representing a variety of clients seeking to invalidate the government's policy of conducting suspicionless searches of laptops and other electronic devices at the international border.

Prior to coming to Berkeley, Professor Crump served as a staff attorney at the ACLU for nearly nine years. Before that, she was a law clerk for Judge M. Margaret McKeown at the United States Court of Appeals for the Ninth Circuit.

Jennifer Daskal joined American University Washington College of Law in 2013 as an Assistant Professor of Law. She teaches and writes in the fields of national security law, criminal law, and constitutional law. From 2009-2011, Professor Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice and, among other things, served on the Secretary of Defense and Attorney General-led Detention Policy Task Force. Prior to joining DOJ, Professor Daskal was senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff (U.S. District Court for the Southern District of New York) from 2001-2002. She spent two years before joining WCL's faculty as a national security law fellow and adjunct professor at Georgetown Law Center.

Professor Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar. Recent and forthcoming publications include *Data's Un-Territoriality* (forthcoming, Yale Law Journal); *After the AUMF*, 5 Harvard National Security Journal 115 (2014) (co-authored with Stephen Vladeck); *Pre-Crime Restraints: The Explosion of Targeted, Non-Custodial Prevention*, 99 Cornell L. Rev. 327 (2014); and *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone*, 171 Penn. L. Rev. 1165 (2013). Professor Daskal has published op-eds in the *New York Times*, *Washington Post*, *International Herald Tribune*, *L.A. Times*, and *Salon.com*, and she has appeared on *BBC*, *CNN*, *C-Span*, *MSNBC*, and *NPR*, among other media outlets. She is an Executive Editor of the national security-focused *Just Security* blog.

Hanni Fakhoury focuses on criminal law, privacy and free speech litigation and advocacy. He's represented clients in criminal and civil government investigations, argued before the Fifth and Ninth Circuits on the constitutionality of surveillance technologies, and written numerous amicus briefs in state and federal courts throughout the country on electronic searches and cybercrime. He's frequently interviewed and quoted by news media organizations including the *Associated Press*, *CBS Evening News*, *CNN*, *Fox News*, *NPR*, the *Wall Street Journal* and the *Washington Post*, and his writings have been published in the *New York Times*, *Slate* and *Wired*. Hanni has testified before the California state legislature on proposed electronic privacy



legislation, is a sought after speaker at domestic and international legal seminars and conferences, and given formal and informal advice to other lawyers on electronic surveillance in criminal cases. Before joining EFF, Hanni worked as a federal public defender in San Diego, where he handled all aspects of criminal litigation including trial and appeal. He still represents federal criminal defendants on appeal as a member of the Northern District of California's Criminal Justice Act panel. Hanni graduated from the University of California, Berkeley with a degree in political science and an honors degree in history. He received his law degree with distinction from Pacific McGeorge School of Law, where he was elected to the Order of Barristers for his excellence in written and oral advocacy.

Ahmed Ghappour is a Visiting Assistant Professor at UC Hastings College of the Law, where he directs the Liberty, Security & Technology Clinic. He is a former computer engineer and is engaged in a number of cross-disciplinary research projects focused on the interplay between emerging technologies, national security and cybersecurity. His clinic litigates constitutional issues that arise in espionage, counterterrorism, and computer hacking cases. He is a member of Chelsea Manning's appellate legal team, lead trial counsel for Barrett Brown, a journalist accused of being the spokesperson for the hacktivist group "Anonymous," and has served as defense counsel in numerous national security cases across the US. Formerly he was a staff attorney at Reprieve UK, where he was habeas counsel for several prisoners detained in Guantanamo Bay without charge.

Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program, which seeks to advance effective national security policies that respect constitutional values and the rule of law. Before coming to the Brennan Center, Ms. Goitein served as counsel to Senator Feingold, Chairman of the Constitution Subcommittee of the Senate Judiciary Committee, and as a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein's writing has been featured in major newspapers including *The New York Times*, *Washington Post*, *Wall Street Journal*, *USA Today*, *LA Times*, *Boston Globe*, *San Francisco Chronicle*, and *Philadelphia Inquirer*. She has appeared on national television and radio shows including the *The Rachel Maddow Show*, *All In with Chris Hayes*, *Up With Steve Kornacki*, the *PBS NewsHour*, and National Public Radio's *Morning Edition* and *All Things Considered*. Ms. Goitein graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit.

Dean Claudio Grossman has served as dean of American University Washington College of Law (AUWCL) since 1995. Under his leadership, AUWCL has become a renowned center for international law, intellectual property, clinical legal education, law and government, and trial advocacy, among other areas for which the school has garnered national and international recognition. AUWCL is also known for its diverse composition of faculty, administrators and students.

A recognized expert in international human rights, Dean Grossman has combined his career in academia with practical experience. He was elected to the United Nations Committee of Torture in 2003 and has served as the Committee's chairperson since 2008, most recently re-elected to that office, for an unprecedented fourth term, in 2014. Previously, Dean Grossman was a member of the Inter-American Commission on Human Rights (IACHR) for eight years (1994-2001) and twice elected its president. He was also the IACHR's Special Rapporteur on the Rights of Women (1996-2000) and Special Rapporteur on the Rights of Indigenous Populations (2000-2001). Additionally, Dean Grossman was responsible for some of the Inter-American system's leading cases involving due process rights, non-discrimination, freedom of expression, the rights of indigenous populations, political rights, and the prohibition of summary executions and forced disappearances, among others.

Dean Grossman is currently the president of the Inter-American Institute for Human Rights (2014-present), where he previously served as board member (2011-2014) and member of the General Assembly (1993-2011). He previously served as president (2003-2007) and board member (2007-2011) of the College of the



Americas (COLAM), an organization encompassing more than 400 universities in the Western Hemisphere. Dean Grossman has authored numerous publications and articles concerning international law, the law of international organizations, human rights and international education. His contributions to those fields have earned him distinctions around the world.

Neema Singh Guliani is a legislative counsel with the American Civil Liberties Union Washington Legislative Office, focusing on national security and immigration issues. Prior to joining the ACLU, she worked in the Chief of Staff's Office at Department of Homeland Security, concentrating on national security and civil rights issues. She has also worked as an adjudicator in the Office of the Assistant Secretary for Civil Rights in the Department of Agriculture and was an investigative counsel with House Oversight and Government Reform Committee, where she conducted investigations related to the BP oil spill, contractors in Iraq and Afghanistan, and the Recovery Act. Ms. Guliani is a graduate of Brown University, where she earned a BA in International Relations with a focus on global security, and she received her JD from Harvard Law School in 2008.

Joseph Lorenzo Hall is the Chief Technologist at the Center for Democracy & Technology (CDT), a Washington, DC-based non-profit organization dedicated to ensuring the internet remains open, innovative and free. Hall's work focuses on the intersection of technology, law, and policy, working carefully to ensure that technology and technical considerations are appropriately embedded into legal and policy instruments. Supporting work across all of CDT's programmatic areas, Hall provides substantive technical expertise to CDT's programs, and interfaces externally with CDT supporters, stakeholders, academics, and technologists.

Prior to joining CDT in 2012, Hall was a postdoctoral research fellow with Helen Nissenbaum at New York University, Ed Felten at Princeton University and Deirdre Mulligan at University of California, Berkeley. Hall received his Ph.D. in information systems from the UC Berkeley School of Information in 2008. His Ph.D. thesis used electronic voting as a critical case study in digital government transparency. In his postdoctoral work, he developed techniques to increase the efficiency and usability of accountability mechanisms in electronic elections. Hall holds master's degrees in astrophysics and information systems from UC Berkeley and was a founding member of the National Science Foundation's ACCURATE Center (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections). He has served as an expert on independent teams invited by the States of California, Ohio and Maryland to analyze legal, privacy, security, usability and economic aspects of voting systems. Hall is the Vice-Chairman of the Board of Directors of the California Voter Foundation, a member of the Board of Directors of the Verified Voting Foundation and a member of the Federal Communications Commission's Computer Security, Reliability, and Interoperability Council (CSRIC) IV. In 2012, Hall received the John Gideon Memorial Award from the Election Verification Network for contributions to election verification.

Jim Harper is a senior fellow at the Cato Institute, working to adapt law and policy to the Information Age in areas such as privacy, cybersecurity, telecommunications, intellectual property, counterterrorism, government transparency, and digital currency. A former counsel to committees in both the U.S. House and the U.S. Senate, he went on to represent companies such as PayPal, ICO-Teledesic, DigitalGlobe, and Verisign, and in 2014 he served as Global Policy Counsel for the Bitcoin Foundation.

A founding member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, Harper co-edited the book *Terrorizing Ourselves: How U.S. Counterterrorism Policy is Failing and How to Fix It*. He has written several *amicus* briefs in Fourth Amendment cases before the U.S. Supreme Court, and is the author of *Identity Crisis: How Identification Is Overused and Misunderstood*. He has been cited by numerous print, Internet, and television media outlets, and has written for the *New York Times*, *Wall Street Journal*, *Politico*, and other leading publications. His scholarly articles have appeared in the *Administrative Law Review*, *Minnesota Law Review*, and *Hastings Constitutional Law Quarterly*.

Harper holds a JD from the University of California – Hastings College of Law.



Professor Orin Kerr is a nationally recognized scholar of criminal procedure and computer crime law. He has authored more than 50 articles, and his scholarship has been cited in over 150 judicial opinions and more than 2000 academic works.

Before joining the faculty at the George Washington University Law School in 2001, Professor Kerr was a trial attorney in the Computer Crime and Intellectual Property Section at the Department of Justice, as well as a Special Assistant U.S. Attorney in the Eastern District of Virginia. He is a former law clerk for Justice Anthony M. Kennedy of the U.S. Supreme Court and Judge Leonard I. Garth of the U.S. Court of Appeals for the Third Circuit.

Professor Kerr has argued cases in the United States Supreme Court and the Third, Fourth, and Sixth Circuits. He has testified six times before congressional committees. In 2013, Chief Justice Roberts appointed Professor Kerr to serve on the Advisory Committee for the Federal Rules of Criminal Procedure.

Professor Kerr has been a visiting professor at the University of Chicago and the University of Pennsylvania, and he served as a scholar-in-residence at the Law Library of Congress from 2012 to 2014. In the summers of 2009 and 2010, he served as special counsel for Supreme Court nominations to Senator John Cornyn on the Senate Judiciary Committee.

The GW Law Class of 2009 awarded Professor Kerr the Law School's teaching award. He posts regularly at the popular blog *The Volokh Conspiracy*. Before attending law school, he earned undergraduate and graduate degrees in mechanical engineering.

David Lieber is a Senior Privacy Policy Counsel for Google based in Washington, D.C. Prior to joining Google, David worked in the E-Commerce & Privacy practice at DLA Piper. David previously served as a Legislative Assistant to Senator Dick Durbin on the Senate Judiciary Committee. He is a graduate of Bates College and Northwestern University School of Law.

E. G. "Gerry" Morris is an Austin, Texas-based criminal defense lawyer, has represented individuals accused of state and federal crimes, both in trial and on appeal. He is Board Certified as a Criminal Law Specialist by the Texas Board of Legal Specialization, and he has been elected by his fellow criminal defense attorneys to leadership positions in both state and national organizations. He served as President of the Texas Criminal Defense Lawyers Association during the 1997-98 term, and is the current President-Elect of the National Association of Criminal Defense Lawyers (NACDL).

The legal community as a whole, through peer rating, has recognized Mr. Morris as being among the top lawyers in Texas. Mr. Morris is listed in the publication *Best Lawyers in America* in both the non-white collar and white collar crime categories, and he was named by *Best Lawyers in America* as Lawyer of the Year in the Austin area for 2012 in the non-white collar crime category. Mr. Morris has also been awarded the coveted "AV" rating by the prestigious Martindale Hubbell Legal Directory and named by *Texas Monthly Magazine* as one of Texas' Super Lawyers in the area of criminal defense.

Perhaps the best-known trial in which Mr. Morris was involved was the "Branch Davidian Trial." In that case Mr. Morris won an acquittal on all charges for his client.

Joseph P. Nacchio's career in the telecommunications industry began at AT&T, where he worked for 26 years and rose to the positions of both President of Business and Consumer Communication Services. He left AT&T in 1997 to become the Chief Executive Officer of Qwest Communications International. In 1999 he also assumed the responsibility of Chairman of the Board of Qwest, a position he held until June 2002. In 2001, he was appointed by President George W. Bush to be Chairman of the National Security



Telecommunications Advisory Committee. Also in 2001, he was asked by former FCC Chairman, Michael Powell, to Chair the Network Reliability and Interoperability Committee.

He has most recently addressed concerns about unlawful surveillance, the overcriminalization of life in America and the widespread abuses in our criminal justice system on *CNBC*, *CBS News*, *Fox Business News*, *The Glen Beck Show*, and the *Wall Street Journal*. Mr. Nacchio is also writing a book about these same concerns and his personal experience with the judicial and federal prison systems.

Mr. Nacchio holds degrees from both New York University and the Massachusetts Institute of Technology.

Gregory T. Nojeim is a Senior Counsel and Director of the Freedom, Security and Technology Project at the Center for Democracy and Technology (CDT), a Washington, D.C. non-profit public policy organization dedicated to keeping the Internet open, innovative and free. Nojeim specializes in protecting privacy in the digital age against intrusion by the U.S. government, and is a recognized expert on the application of the Fourth Amendment to electronic surveillance in the national security, intelligence and criminal arenas. He spearheaded CDT's efforts to promote judicial supervision of surveillance of Americans' private telephone and e-mail conversations in connection with legislation to update the U.S. Foreign Intelligence Surveillance Act in 2008.

He is currently a leader in CDT's cybersecurity work, testifying in both the House and Senate on the impact of cybersecurity proposals on privacy, civil liberties, and technology innovation. He is the author of "Cybersecurity and Freedom on the Internet," published in 2010 in the *Journal of National Security Law and Policy*. Nojeim is also deeply involved in a multi-year, broad-based project to update the Electronic Communications Privacy Act.

As Co-Chair of the Coordinating Committee on National Security and Civil Liberties of the American Bar Association's Section on Individual Rights and Responsibilities, he was one of the lead drafters of the ABA's 2007 policy on the state secrets privilege.

Prior to joining CDT in May 2007, Nojeim was the Associate Director and Chief Legislative Counsel of the ACLU's Washington Legislative Office. He graduated from the University of Rochester in 1981 with a B.A. in Political Science, and he received his J.D. from the University of Virginia in 1985.

Norman L. Reimer is the Executive Director of the National Association of Criminal Defense Lawyers (NACDL), the nation's preeminent criminal defense bar association. Since joining NACDL, Norman Reimer has overseen a significant expansion of the Association's educational programming and policy initiatives, cultivated external support and launched a major capital campaign. Mr. Reimer also serves as the publisher of NACDL's acclaimed *Champion* magazine.

Prior to assuming this position, he practiced law for 28 years. A criminal defense lawyer throughout his career, Mr. Reimer is also a recognized leader of the organized bar, and a spokesperson on behalf of reform of the legal system. He is a past president of the New York County Lawyers' Association (NYCLA); in his work at NYCLA, he played a pivotal role in undertaking litigation against the State and City of New York that upheld the right of a bar association to sue on behalf of indigent litigants and resulted in a judicial decision declaring New York's under-funding of indigent defense services unconstitutional. Mr. Reimer has also served as a delegate to both the American Bar Association House of Delegates and the New York State Bar Association House of Delegates. Mr. Reimer has played leading roles on several other reform efforts on a range of issues including mandatory recording of custodial interrogations, a moratorium on death penalty prosecutions, judicial independence, preservation of *habeas corpus*, and collateral consequences of criminal convictions.



During his tenure at NACDL, he has participated in numerous amicus curiae briefs on issues related to indigent defense reform, judicial independence and GPS tracking.

Norman Reimer taught Trial Practice as an Adjunct Professor of Law at New York Law School from 1990 until 2004. He received his B.A. *cum laude* from New York University's Washington Square College and his J.D. with honors in criminal law from New York University School of Law.

Jeffrey Rosen is the President and Chief Executive Officer of the National Constitution Center, the only institution in America chartered by Congress "to disseminate information about the United States Constitution on a non-partisan basis." Housed in a Pei-Cobb building across from Independence Hall and the Liberty Bell in Philadelphia, the Constitution Center engages millions of citizens as an interactive museum, national town hall, and headquarters for civic education.

Rosen is also a professor at The George Washington University Law School, as well as a Contributing Editor for *The Atlantic*. He is a nonresident senior fellow at the Brookings Institution, where he explores issues involving the future of technology and the Constitution. He has recorded a lecture series for the Teaching Company's Great Courses on Privacy, Property, and Free Speech: Law and the Constitution in the 21st Century. Since 2000, he has served as a moderator at The Aspen Institute, where he conducts seminars and panels on technology and the Constitution, privacy, and free speech and democracy.

He is a highly regarded journalist whose essays and commentaries have appeared in the *New York Times Magazine*, on *National Public Radio*, and in *The New Yorker*, where he has been a staff writer. The *Chicago Tribune* named him one of the 10 best magazine journalists in America and a reviewer for the *Los Angeles Times* called him "the nation's most widely read and influential legal commentator." He received the 2012 Golden Pen Award from the Legal Writing Institute for his "extraordinary contribution to the cause of better legal writing."

Rosen is the author of several books including *The Supreme Court: The Personalities and Rivalries that Defined America*; *The Most Democratic Branch: How the Courts Serve America*; *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*; and *The Unwanted Gaze: The Destruction of Privacy in America*. His most recent book, as co-editor, is *Constitution 3.0: Freedom and Technological Change*. Books about Supreme Court Justice Louis Brandeis and President William Howard Taft are forthcoming.

Rosen is a graduate of Harvard College; Oxford University, where he was a Marshall Scholar; and Yale Law School.

Theodore "Ted" Simon is an attorney in private practice in Philadelphia, Pa., where he has based a local, national and international practice for the last 40 years. He has obtained reversals in the U.S. Supreme Court and in the Pennsylvania Supreme Court. Simon has been a NACDL member since 1979 and was sworn in as NACDL's 57th President on August 2, 2014, in Philadelphia, Pa. He is also a Trustee of the Foundation for Criminal Justice and was Chair of the well-attended, highly-successful and inspirational 2014 Foundation for Criminal Justice Awards Dinner, which was held August 1, 2014, at the National Constitution Center.

In addition to representing individuals and corporations in state and federal trial and appellate proceedings, Simon is a leading authority on the representation of Americans abroad and securing their outright release from custody, as well as on the application of prisoner transfer treaties here and abroad, achieving remarkable success in obtaining the transfer of numerous foreign nationals. He has also successfully defended international extradition requests. A frequent speaker at legal seminars across the nation on a wide variety of pre-trial, trial, sentencing, and post-trial criminal law issues, Simon has made numerous appearances on



The Today Show, Good Morning America, Early Show, CNN, ABC's 20/20, Primetime, NBC's Dateline, Larry King Live, Court TV, Geraldo Live, Crossfire, The Abrams Report, and The Oprah Winfrey Show (as well as all of the major networks and cable outlets). Immediately following the 2000 presidential election, Mr. Simon hosted his own daily cable TV show, which analyzed various current legal issues. Additionally, Mr. Simon, as a result of his combined legal and communication skills and long-standing relationships with the media, is a much sought after legal and media consultant.

Kenneth Wainstein is Chair of the white-collar group at Cadwalader, where he focuses his practice on corporate internal investigations and civil and criminal enforcement proceedings. Mr. Wainstein spent over 20 years in a variety of law enforcement and national security positions in the government. Between 1989 and 2001, he served as an Assistant U.S. Attorney in both the Southern District of New York and the District of Columbia, where he handled criminal prosecutions ranging from public corruption to gang prosecution cases and held a variety of supervisory positions, including Acting United States Attorney. In 2001, he was appointed Director of the Executive Office for U.S. Attorneys, where he provided oversight and support to the 94 U.S. Attorneys' Offices. Between 2002 and 2004, Mr. Wainstein served as General Counsel of the Federal Bureau of Investigation and then as Chief of Staff to Director Robert S. Mueller III. In 2004, he was appointed and then confirmed as United States Attorney for the District of Columbia, where he had the privilege to lead the largest United States Attorney's Office in the country. In 2006, the U.S. Senate confirmed him as the first Assistant Attorney General for National Security. In that position, he established and led the new National Security Division, which consolidated DOJ's law enforcement and intelligence activities on counterterrorism and counterintelligence matters. In 2008, after 19 years at the Justice Department, Mr. Wainstein was named Homeland Security Advisor by President George W. Bush. In this capacity, he coordinated the nation's counterterrorism, homeland security, infrastructure protection, and disaster response and recovery efforts. He advised the President, convened and chaired meetings of the Cabinet Officers on the Homeland Security Council, and oversaw the inter-agency coordination process for homeland security and counterterrorism programs.

Eric Wenger serves as the Director for Cybersecurity and Privacy on Cisco's Global Government Affairs team in Washington. Mr. Wenger leads Cisco's work on cybersecurity policy globally, as well as on privacy matters relating to the U.S. government, including on issues related to government surveillance and the Internet of Everything.

Mr. Wenger came to Cisco from Microsoft, where he served as Policy Counsel in the Legal and Corporate Affairs Department. His portfolio covered a range of cybersecurity, cybercrime, data breach, and privacy issues, including efforts to reform U.S. surveillance laws.

Prior to Microsoft, Mr. Wenger worked as a Trial Attorney in the Department of Justice's Computer Crime and Intellectual Property Section. He also worked as an attorney in the Federal Trade Commission's Bureau of Consumer Protection and an Assistant Attorney General in New York State, where he started the first statewide law enforcement unit in the country focused on e-commerce.



Appendix B — Program

Friday, April 3 | 8:30 am - 4:00 pm | Reception to Follow

American University Washington College of Law

4801 Massachusetts Avenue NW, Washington, DC 20016 | Room 603

8:30 - 9:00 Registration and Breakfast

9:00 - 9:20 Introductory Remarks

Dean Claudio Grossman, *Dean of American University Washington College of Law and the Raymond I. Geraldson Scholar for International and Humanitarian Law*

Theodore Simon, *President, National Association of Criminal Defense Lawyers*

9:20 - 11:00 PANEL 1: New Developments in Surveillance Technology: How the Government Collects, Searches, Stores, and Shares Information

MODERATOR:

Jennifer Daskal, *Assistant Professor of Law, American University Washington College of Law*

DISCUSSANTS:

Catherine Crump, *Assistant Clinical Professor of Law; Associate Director, Samuelson Law, Technology and Public Policy Clinic at the UC Berkeley School of Law*

Elizabeth Goitein, *Co-Director of the National Security Project, Brennan Center for Justice at NYU Law School*

Joseph Lorenzo Hall, *Chief Technologist, Center for Democracy & Technology*

Eric Wenger, *Director of Cybersecurity and Privacy Policy for Global Government Affairs, Cisco Systems*

11:00 - 11:10 Break

11:10 - 12:50 PANEL 2: Challenges to the System: Prosecutors, Judges, and Defense Attorneys in the Digital Age

MODERATOR:

E.G. "Gerry" Morris, *President-Elect National Association of Criminal Defense Lawyers*

DISCUSSANTS:

Hanni Fakhoury, *Senior Staff Attorney, Electronic Frontier Foundation*

Neema Singh Guliani, *Legislative Counsel, American Civil Liberties Union*

Jim Harper, *Senior Fellow, CATO Institute*

Orin Kerr, *Fred C. Stevenson Research Professor of Law, George Washington University Law School*

12:50 - 2:00 Lunch and a Conversation with Joseph P. Nacchio, *Former Chairman and CEO, Qwest Communications International*

Norman L. Reimer, *Executive Director, National Association of Criminal Defense Lawyers*





2:00 - 2:10 **Break**

2:10 - 3:50 **PANEL 3: Law and Policy: A Path Forward for the Constitution,
Courts, Congress, and Law Enforcement**

MODERATOR:

Jeff Rosen, *President and CEO, National Constitution Center;
Professor of Law, George Washington University Law School*

DISCUSSANTS:

Ahmed Ghappour, *Visiting Professor, UC Hastings College of the Law;
Director, Liberty, Security and Technology Clinic*

David Lieber, *Senior Privacy Policy Counsel, Google*

Greg Nojeim, *Senior Counsel and Director, Freedom, Security and
Technology Project, Center for Democracy and Technology*

Kenneth Wainstein, *Partner, Cadwalader, Wickersham & Taft LLP; Former Homeland
Security Advisor; Former Assistant Attorney General for National Security, DOJ;
Former United States Attorney for the District of Columbia*

3:50 **Closing remarks and reception**

SPONSORED BY

The National Association of Criminal Defense Lawyers

The Foundation for Criminal Justice

The American University Washington College of Law

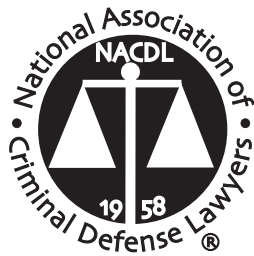
Criminal Law Practitioner







This publication is available online at
www.nacdl.org/FourthAmendmentInTheDigitalAge



For more information contact:

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

1660 L Street NW, 12th Floor

Washington, DC 20036

Phone: 202-872-8600

www.nacdl.org

This publication is available online at

www.nacdl.org/FourthAmendmentInTheDigitalAge