NATIONAL SECURITY, SURVEILLANCE TECHNOLOGY AND THE LAW
Co-sponsored by Georgetown Law and the Federal Judicial Center

June 1 – 2, 2015

Georgetown Law
Gewirz Center, 12th Floor
120 F Street, NW
Washington, D.C. 20001

Monday, June 1, 2015

8:00 am – 8:40 am: **Continental Breakfast**

8:40 am – 8:45 am: **Welcome and Introduction**
William M. Treanor, *Dean, Georgetown Law*
John Cooke, *Deputy Director, Federal Judicial Center*

***Session 1*—Interception and Location Tracking**
Description: Title III provides the framing for the collection of telephone content. With mobile technologies, law enforcement has new tools available to collect content (e.g., remotely activating the device's microphone or camera), locate cell phones (e.g., Stingray), and follow the movement of mobile telephones (e.g., GPS chips or trunk identifier information). Understanding how these technologies work is critical to determining under what conditions warrants are required, whether the evidence presented is sufficient to grant them, and whether the scope of the request is appropriate for the type of information that law enforcement may expect to obtain. Computer scientists will present the technologies in question and demonstrate their potential. Following the technology discussion, the panel will address the current law and the Fourth Amendment questions that parallel the evolution of these new technologies.

8:45 am – 10:15 am: **Technology Module**
Professor Steven M. Bellovin, *Professor of Computer Science, Columbia University*
Christopher Soghoian, *Principal Technologist and Senior Policy Analyst, ACLU*

10:15 am – 10:30 am: **Coffee Break**

10:30 am – 12:00 pm: **Legal Architecture and Doctrinal Implications**
Hanni Fakhoury, *Senior Staff Attorney, Electronic Frontier Foundation*
Nathan Judish, *Senior Counsel, Computer Crimes and Intellectual Property Section, U.S. Department of Justice*
Judge M. Margaret McKeown, *U.S. Court of Appeals for the Ninth Circuit*
Judge David B. Sentelle, *U.S. Court of Appeals for the D.C. Circuit*
Professor David Cole, *Professor of Law, Georgetown Law* (moderator)

12:00 pm – 12:15 pm: **Lunch Buffet**

***Session 2*—The Internet of Things**
Description: The Internet of Things (IoT) describes the network of physical items embedded with electronics, software, and sensors, which allows consumers to optimize services associated with the goods. The items are stand-alone objects, which are incorporated into the Internet infrastructure. The range of items included in the IoT is vast: automobiles, health monitors, biochips on farm animals, environmental monitoring devices, refrigerators, and home energy management represent just a few of the many devices involved. The advent of Smart technologies means many things, not least of which is a dramatic increase in information available. Philip Reitinger is uniquely placed to address what the IoT means in the context of law enforcement and national security. He served as Deputy Under Secretary of the National Protection and Programs Directorate and the Director of the National Cyber Security Center at the Department of Homeland Security; Executive Director for the Department of Defense Cyber Crime Center; and Deputy Chief of the Computer Crime and Intellectual Property Section of the Department of Justice's Criminal Division. Mr. Reitinger was a Senior Security Strategist with Microsoft Corporation's Trustworthy Computing Security Team and Senior Vice

President and Chief Information Security Officer at Sony. He is now a Senior Associate at the Center for Strategic and International Studies.

12:15 pm – 1:15 pm: **Luncheon Keynote Address—*The Internet of Things*,** Philip R. Reitinger, *Senior Associate, Strategic Technologies Program, Center for Strategic and International Studies*

Introduction: Professor Laura K. Donohue, *Professor of Law, Georgetown Law; Director, Georgetown Center on National Security and the Law; Director, Georgetown Center on Privacy and Technology*

Session 3—Computer Architecture and Remote Access

Description: The Department of Justice is seeking a change to the Federal Rules of Criminal Procedure to provide it with the ability to obtain search warrants to access computers from remote locations. It argues that new rules are required to allow law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing techniques. Digital rights groups respond that the request for an expansion to Rule 41 raises concern about Internet Security and Fourth Amendment protections against unreasonable search and seizure. The Advisory Committee on the Criminal Rules initially considered the proposed rule in 2013. A revised proposal was published for public comment in 2014, after which the Committee received written comments and oral testimony. This past March the Committee approved the proposal, which is currently pending further review before the Standing Committee on Practice and Procedure. This session will look at both individual computer architecture as well as network architecture in the context of the current use of remote access warrants and requests for an alteration to Rule 41.

1:15 pm – 2:45 pm: **Technology Module**

Bruce Schneier, *Fellow, Berkman Center for Internet & Society, Harvard Law School*
Lewis Shepherd, *Director, Microsoft Institute for Advanced Technology in Governments*

2:45 pm – 3:00 pm: **Coffee Break**

3:00 pm – 4:30 pm: **Legal Architecture and Doctrinal Implications**

Alan Butler, *Senior Counsel, Electronic Privacy Information Center*
Judge Stephen W. Smith, *U.S. District Court for the Southern District of Texas*
Michael Stawasz, *Deputy Chief for Computer Crime, Computer Crime & Intellectual Property Section, U.S. Department of Justice*
Professor Orin Kerr, *Fred C. Stevenson Research Professor of Law, George Washington University Law School*

Tuesday, June 2, 2015

Session 4—Metadata and Social Network Analytics

Description: On May 24, 2006, the Foreign Intelligence Surveillance Court (FISC) approved an FBI application for an order, pursuant to 50 U.S.C. § 1861, requiring Verizon to turn over all telephony metadata to the National Security Agency. The Court subsequently approved similar applications for all major U.S. telecommunication service providers. Since that time, FISC has issued orders renewing the bulk collection program more than forty times. Almost all of the information obtained related to the activities of individuals who were not the subjects of any investigation. The revelation of the bulk data collection program spurred public debate and led to an announcement by President Obama in January 2014 that the NSA would replace the program with a new approach. This session will begin with a presentation by prominent technologists in academia and industry, discussing the contours of social network analysis and metadata collection. Section 215 of the USA PATRIOT Act, under which the NSA bulk collection of telephony metadata was conducted, is set to expire June 1, 2015. Following the panel, there will be a brief update on Congress's action. The legal and doctrinal panel that follows will address the statutory and constitutional aspects of bulk collection and the §215 debate.

8:30 am – 9:45 am: **Technology Module**

Jonathan Mayer, *Center for Internet and Society, Stanford Law School; Graduate Fellow, Security Laboratory, Department of Computer Science, Stanford University*
Joseph Lorenzo Hall, *Chief Technologist, Center for Democracy & Technology*

9:45 am – 10:00 am: **Congressional Update on § 215**

Julian Sanchez, *Senior Fellow, Cato Institute*

10:00 am – 10:15 am: **Coffee Break**

10:15 am – 11:45 am: **Legal Architecture and Doctrinal Implications**
Judge John D. Bates, *U.S. District Court for the District of Columbia*
Judge Leonie M. Brinkema, *U.S. District Court for the Eastern District of Virginia*
Judge Beryl A. Howell, *U.S. District Court for the District of Columbia*
Julian Sanchez, *Senior Fellow, Cato Institute*
Professor Viet Dinh, *Professorial Lecturer, Georgetown Law* (moderator)

11:45 am – 12:00 pm: **Lunch Buffet**

***Session 5*—Classification and Case Management**
Description: Judicial independence and national security meet when a federal court is called upon to preside over national security cases. Criminal prosecutions for terrorism or espionage, civil challenges to government conduct, and even civil actions between private parties can present our courts with the challenge of providing justice and protecting national security at the same time. The Justice Department's Litigation Security Group helps courts properly protect classified information that becomes part of national security litigation. Classified information security officers provided by the Litigation Security Group also assist court staff and private attorneys with the process of obtaining security clearances. The lunchtime discussion will cover the state secrets privilege, the Classified Information Procedures Act (CIPA), sensitive compartmented information facilities (SCIFs), and more, including both questions and answers from judges in attendance.

12:00 pm – 1:00 pm: **Luncheon Discussion—*The National Security Docket,*** Tim Reagan, *Senior Research Associate, Federal Judicial Center;* Daniel O. Hartenstine, *Security Specialist, Litigation Security Group, U.S. Department of Justice.*
Introduction: Professor Laura K. Donohue, *Professor of Law, Georgetown Law; Director, Georgetown Center on National Security and the Law; Director, Georgetown Center on Privacy and Technology*

***Session 6*—Cloud Computing and Global Communications**
Description: In July 2008 Congress passed the FISA Amendments Act to address the impact of rapidly-evolving global communications systems on foreign intelligence collection. The primary concern was that communications outside the United States, which previously would have been governed by Executive Order 12333, were being pulled into the more rights-protective framing of FISA because of how the Internet works. Section 702 focused on the collection of non-U.S. persons' electronic communications, where such individuals were believed to be outside the United States. Sections 703 and 704 emphasized the collection of U.S. persons' information when they were believed to be outside domestic borders. In June 2013 the Snowden documents suggested that the NSA was using Section 702 to obtain significant amounts of U.S. persons' communications, both inside and outside the United States, by nature of how the order, issued by FISC, operated. Slides detailing PRISM, a program that obtained information from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple, and upstream collection, which entailed obtaining global communications as they transited Internet backbone facilities, suggested significantly deeper collection than had previously been understood. The information obtained from Section 702 collection can be used in criminal prosecution, as well as for foreign intelligence purposes. The technology module for this session will focus on the global communications infrastructure and consider how cloud computing works. The following panel will consider the legal architecture and doctrinal implications.

1:00 pm – 2:30 pm: **Technologist Presentation**
Professor Steven M. Bellovin, *Professor of Computer Science, Columbia University*
Barton Gellman, *Senior Fellow, The Century Foundation*

2:30 pm – 4:00 pm: **Legal Architecture and Doctrinal Implications**
Robert S. Litt, *General Counsel, Office of the Director of National Intelligence*
Marc Rotenberg, *President and Executive Director, Electronic Privacy Information Center*
Richard Salgado, *Director for Information Security and Law Enforcement, Google, Inc.*

Professor Laura K. Donohue, *Professor of Law, Georgetown Law; Director, Georgetown Center on National Security and the Law; Director, Georgetown Center on Privacy and Technology* (moderator)

4:00 pm – 4:15 pm: **Summary and Insights**
Judge Cornelia T.L. Pillard, *U.S. Court of Appeals for the D.C. Circuit*

4:15 pm: **Workshop concludes**