

FOR IMMEDIATE RELEASE

Contact: Merissa Blum, 215-409-6645
mblum@constitutioncenter.org

LEADING SCHOLARS AND THOUGHT LEADERS RELEASE WHITE PAPERS ON IMPACT OF NEW TECHNOLOGIES ON PRIVACY, SURVEILLANCE, CYBERSECURITY, AND LAW ENFORCEMENT

Authors will convene to discuss the white papers at the National Constitution Center on Wednesday, May 10, 2017

Philadelphia, PA (May 8, 2017) – The National Constitution Center released a white paper series – entitled “[A Twenty-First Century Framework for Digital Privacy](#)” – addressing the impact of new technologies on privacy rights, government surveillance, cybersecurity, and law enforcement. The papers examine the challenges that new technologies pose to the existing legal framework and propose solutions. The authors – which include some of the country’s top scholars and thought leaders on the issues of national security, law enforcement, and digital privacy – will gather at the National Constitution Center on Wednesday, May 10 at 6:30 p.m. to discuss their findings and explore the future of the Fourth Amendment in the digital age.

“The National Constitution Center is thrilled to be able to bring together such a diverse group of scholars and thought leaders to discuss one of most important legal challenges of the digital age—how to protect privacy and security in the era of cloud computing,” said Jeffrey Rosen, President and CEO of the National Constitution Center. “This new white paper series reflects the Constitution Center’s commitment to presenting the best available arguments on all sides of the constitutional issues at the center of American life. It will help us address the crucial challenge of how best to translate the Constitution and key privacy laws in light of new technologies.”

Synopses of each white paper are included below. Authors and titles for each paper include:

- **Jennifer Daskal**, Associate Professor of Law at American University: “[Whose Law Governs in a Borderless World? Law Enforcement Access to Data Across Borders](#)”
- **Jim Harper**, Vice President of the Competitive Enterprise Institute: “[Administering the Fourth Amendment in the Digital Age](#)”
- **David Kris**, former Assistant Attorney General for National Security: “[Digital Divergence](#)”
- **Neil Richards**, Thomas and Karole Green Professor of Law at Washington University: “[Secret Government Searches and Digital Civil Liberties](#)”
- **Christopher Slobogin**, Milton R. Underwood Chair in Law at Vanderbilt University: “[Policing and The Cloud](#)”

White paper authors Harper, Kris, Daskal, and Slobogin will convene for the event on Wednesday, May 10, at the National Constitution Center. The program will be moderated by Thomas Donnelly, National Constitution Center Senior Fellow for Constitutional Studies, and will include a keynote speech entitled “What Would Brandeis Do in the Digital Age?” by Jeffrey Rosen, National Constitution Center President and CEO. The event will be livestreamed on the National Constitution Center’s website at constitutioncenter.org/live.

WHITE PAPER SYNOPSES

Title: [“Whose Law Governs in a Borderless World? Law Enforcement Access to Data Across Borders”](#)

Author: Jennifer Daskal, Associate Professor of Law at American University

Synopsis: It is not simple to translate the traditional rules governing searches and seizures to the world of digital evidence. There are, after all, key—and highly relevant—distinctions between digitalized evidence and its more tangible counterparts. Data can move across borders and around the world instantly, can be held in multiple places at once, and can be accessed remotely from across the globe. Our failure to adequately account for these differences is having increasingly negative consequences for our security, our privacy, and our economy. Today, legal rules covering government access to data focus on data location. A better rule would shift the focus to a variety of other factors, including target location and nationality, the location of the provider, and the strength of the government’s interest. These factors better reflect the interest at stake in cross-border data dispute, including privacy, security, and sovereignty.

Title: [“Administering the Fourth Amendment in the Digital Age”](#)

Author: Jim Harper, Vice President of the Competitive Enterprise Institute

Synopsis: Modern Fourth Amendment jurisprudence is a muddle, and it is sorely challenged by advances in information technology. Our entry into the Information Age demands a new, higher respect for data, information, and communications as common law property. Courts should reject an approach to the Fourth Amendment that focuses on society’s “reasonable expectations of privacy” and should instead adopt one that hues closely to the Fourth Amendment’s text and recognizes data, information, and communications as a key form of property. Simply put, if there was a “search” or “seizure,” if it was of protected things, and if it was unreasonable, then the Fourth Amendment has been violated. That is how to administer the Fourth Amendment. This approach would place judges back in the familiar position of applying the law to the facts of a specific case.

Title: [“Digital Divergence”](#)

Author: David Kris, former Assistant Attorney General for National Security

Synopsis: This paper addresses the effects of advances in technology on statutory and constitutional law and challenges the view that balancing privacy and security is a zero-sum game. Technological advances increase (what the paper calls) “digital divergence,” making it easier for informed and motivated individuals, groups, and governments to defeat surveillance, commit misconduct, and avoid attribution, but harder for everyone else to protect against such misconduct and to control their own personal data. Digital network technology has brought enormous benefits, but digital divergence threatens *both* privacy *and* security. This trend has the potential to upset many of our established rules and practices—not in a single burst of new law created intentionally by elected officials, but through a rapid and radical transformation of the environment underlying the old laws fueled by commercial motives.

Title: [“Secret Government Searches and Digital Civil Liberties”](#)

Author: Neil Richards, Thomas and Karole Green Professor of Law at Washington University

Synopsis: This paper explores the issue of “secret government searches”—namely, instances of government surveillance that remain a secret to the search target. It attempts to put the rise of secret government searches into context—historical, technological, and most importantly constitutional—and argues that these searches are unprecedented, historically and technologically, and inconsistent with key constitutional values, including freedom of thought, freedom of expression, and freedom from unreasonable searches and seizures.

Title: [“Policing and The Cloud”](#)

Author: Christopher Slobogin, Milton R. Underwood Chair in Law at Vanderbilt University

Synopsis: It is now a commonplace that virtually everything we do is memorialized on databases. These databases—the servers of Google, Netflix, and Apple; the memory banks of phones, closed circuit cameras, “smart cars,” and satellites; the computers in commercial establishments and government agencies—track an astonishing range of our intimate daily activities, including financial transactions, internet connections, travel routes, tax information, and medical treatment. But when should the government be able to gain access to this wealth of personal information for law enforcement and national security purposes? Private and government databases are full of information that can enhance law enforcement’s ability to detect and investigate crime and terrorism. However, given the personal nature of the information stored in The Cloud, law enforcement shouldn’t be able to access it at will. Instead, the challenges of the digital age require an approach that is sensitive to the context of the specific government action or request. While a warrant may not be appropriate in all circumstances, a mere subpoena may not be sufficient, either. In crafting the right approach, the goal should be to construct rules that will allow government to harness The Cloud’s investigative potential, while also limiting the opportunities for government abuses.

The National Constitution Center and the authors of these papers maintained editorial independence during the production of “A Twenty-First Century Framework for Digital Privacy.” The series was produced with support from Microsoft.

About the National Constitution Center

The [National Constitution Center](#) in Philadelphia inspires citizenship as the only place where people across America and around the world can come together to learn about, debate, and celebrate the greatest vision of human freedom in history, the U.S. Constitution. A private, nonprofit organization, the Center serves as America’s leading platform for constitutional education and debate, fulfilling its Congressional charter “to disseminate information about the U.S. Constitution on a nonpartisan basis.” As the **Museum of We the People**, the Center brings the Constitution to life for visitors of all ages through interactive programs and exhibits. As **America’s Town Hall**, the Center brings the leading conservative and liberal thought leaders together to debate the Constitution on all media platforms. As a center for **Civic Education**, the Center delivers the best educational programs and online resources that inspire, excite, and engage citizens about the U.S. Constitution. For more information, call 215-409-6700 or visit [constitutioncenter.org](#).

###