Nebraska Law Review

Volume 96 | Issue 2 Article 2

2017

State, Local, and Regional Issues in Cybersecurity: Symposium Introduction

Justin (Gus) Hurwitz
University of Nebraska College of Law, ghurwitz@unl.edu

Justin (Gus) Hurwitz*

State, Local, and Regional Issues in Cybersecurity: Symposium Introduction

Cybersecurity is one of the more difficult and urgent issues of the day. It is an issue that touches almost every aspect of modern life. Recent years have seen major cybersecurity incidents affect national security, our political process, major government institutions, companies of every size throughout our economy, critical infrastructure, banking, consumer electronics, and, of course, consumers themselves. Examples of each of these feature so prominently in the news that they barely need citation: OPM, Sony, Target, concerns about the 2016 election, disclosure of NSA hacking tools, attacks on the banking sector's SWIFT network, ransomware attacks against hospitals, DDoS attacks against the Internet's Domain Name System using networks of hundreds of thousands (if not millions) of compromised consumer-owned, Internet-connected devices. This list could fill several pages—and that is with only well-publicized, high-profile incidents—the tip of the cybersecurity iceberg.

Most discussion about cybersecurity law and policy focuses on issues as they occur at a national or supra-national level. This is unsurprising: the nexus of issues that define cybersecurity have long fallen within the ambit of federal regulation and national security, and most sophisticated cybersecurity actors have long been those operating at the nation–state scale. But much of what happens in cybersecurity occurs at the subnational level. The targets of cybersecurity incidents are usually local actors, as are the first responders; state and local governments often face cybersecurity concerns equal to those of national-level government; much of current "cybersecurity law" exists at the state level; and most critical infrastructure is owned by firms operating within, and largely regulated by, individual states.

In March 2017, the University of Nebraska College of Law's Space, Cyber, and Telecommunications Law Program, in conjunction with

[*] Justin (Gus) Hurwitz is an Assistant Professor of Law at the University of Nebraska College of Law and Co-Director of the Space, Cyber, and Telecommunications Law Program.

the *Nebraska Law Review*, convened a conference to discuss cybersecurity issues at the state, local, and regional level. The present volume of the *Review* includes a symposium comprising contributions from that conference's participants.

Organizing such a conference is a daunting task. Cybersecurity is an inherently and dauntingly inter- and intra-disciplinary field. This follows from the architecture and purpose of the Internet: the Internet is an "internetwork," designed to network networks of computers together. The practical effect of this architecture is to break down silos, bringing conduct and regulation that has historically been understood as falling narrowly within one domain into contact with other conduct and regulation. At a technical level, to a surprising extent the same technologies—from computers to operating systems to networking protocols—are used today by consumers, corporations, infrastructure, civilian government, and the national-security community. Yet the needs of each of these communities is different. (Or, perhaps, they aren't—In an interconnected environment do consumers need as good security as the NSA? Can the NSA really have better security than consumers?)

The conference brought together over a dozen academics and practitioners from a range of fields. The day's discussion included three panels and a keynote address by Michael Garcia, of the National Governors Association's Homeland Security & Public Safety Division. The morning's discussion focused on issues faced by law enforcement and the role challenges of critical infrastructure; the afternoon's discussion featured a wide-ranging discussion of government and governance—particularized discussion of the cybersecurity challenges faced by state and local government, and generalized discussion of what governance structures work best in dealing with these problems. A brief discussion of each panel and of related contributions follows below.

But first, a few thanks and acknowledgements are in order. This conference would not have happened without the support and assistance of Elsbeth Magilton, Executive Director of the Space, Cyber, and Telecommunications Law Program, and administrative support of Bambi King. Similarly, my co-director, Matt Schaefer, provided invaluable support in designing the conference early on and offering input as it developed. The editors of the *Nebraska Law Review* took a risk on this event, devoting an issue to the symposium and topic, as well as suffering through my own disorganization: my thanks in particular to Taylor Fritsch and Kelsey E.B. Knoer for giving the event the green light, and to Chelsea Avent and Taylor Cammack for working with me to make it happen. Attorney General Doug Peterson and Dean Richard Moberly both provided a warm welcome to conference attendees and have consistently offered greatly appreciated support for and interest in the work of the Space, Cyber, and Telecommunications Law

Program. Last, but not least, thanks go to all of the participants and attendees who joined us for the conference.

The first panel of the day focused on issues facing law enforcement. The panel was moderated by Dan Birdsall of the Nebraska Attorney General's office. It featured contributions from Jennifer Brobst (SIU Law), Catherin Crump (UC Berkeley), Dennis Kamph (Attorney-Investigator, DOJ), and Mike Norris (Nebraska AUSA). The discussion focused on the challenges faced by law enforcement in responding to cybercrime. In particular, it focused on the challenges faced by local law enforcement in responding to crimes that occur on a national scale but in which the impact is felt on a local scale; the challenges facing local law enforcement in investigating and prosecuting even moderately sophisticated online crimes; the realities of coordinating between local, state, and federal law enforcement entities; the definitional challenges of understanding the nature of "harm" in the cyber context; and the tools available to law enforcement. The panel featured particularly insightful discussion about the challenges of investigating crimes in which the location of the perpetrator is unknown. A key investigation that was a predecessor to Operation Playpen and the 2016 amendments to the *Federal Rules of Criminal Procedure*'s Rule 41 was based out of Nebraska—Mike Norris discussed how that investigation differed from, and offered a more circumspect approach than (my gloss; not Mike's words), Operation Playpen, and Catherine Crump offered the "defense counsel's perspective" on these changes, offering a critical understanding of these rules.

This symposium volume includes a contribution from Professor Brobst that offers an important discussion of interpersonal cybercrime and the costs that victims can face when availing themselves of legal recourse. Concerns about publicizing their injury in an Internet-connected and searchable judicial system can worsen a victim's existing injury and discourage engagement with the legal system; these concerns expose conflicts between ensuring justice and longstanding views of the importance of judicial transparency. Professor Brobst's Article explores and struggles with these issues, offering guidance for courts and the legal system to balance the needs of victims and the judiciary.

I moderated the second panel of the day, which focused on critical infrastructure. Participants included Paul Diamond (CenturyLink), Ezra Glanzer (Washington National Guard), Pete Sakaris (President of ISS, Inc.; former FBI), Scott Shackelford (IU Bloomington, Business), and Bryan Tuma (Assistant Director, Nebraska Emergency Management Authority). As is often the case with discussions of critical infrastructure, the discussion was as scary as it was informative. The task of securing critical infrastructure—the myriad invisible systems, platforms, and technologies that everyone in the country depends on every day in every aspect of their lives—is daunting; the consequences if its security is compromised are severe; and the responsibility of and capabilities to secure it or respond to compromises are unclear. These challenges are particularly difficult in a context where much critical infrastructure simultaneously is privately owned and operated at a scale that rivals many governments, and in which ex post facto legal remedies can do little to mitigate the harms that result from a security compromise. The fascinating part of this discussion was the interaction between panelists who generally think at national- and state-level scales. The key takeaway from the discussion may well have been that the best hope for addressing critical infrastructure cybersecurity lies not in the law or technology but in relationships between various actors in the infrastructure community, ensuring that operators know their peers and colleagues throughout the community so that they are in a position to dynamically identify and respond to the evolving threat landscape.

This symposium volume includes a contribution from cybersecurity tour de force Scott Schackelford. Scott and his colleagues offer a study of Russian efforts to compromise critical infrastructure in the United States—including voting systems during the 2016 election—and the Ukraine, and evaluation of current and future efforts in the United States to protect against such attacks. In the context of the conference, this Article presents an important study and reminder of the complex hierarchical relationships that exist in the cybersecurity context: a foreign nation compromising state and local infrastructure in order to influence U.S. politics.

The lunchtime keynote was presented by Michael Garcia on behalf of the National Governors Association (NGA). Every year the chair of the NGA selected a primary area of focus—the Chair's Initiative. For 2016–2017, Virginia Governor Terry McAuliffe, the current chair, has identified "States Confront the Cyber Challenge" as this initiative. Michael presented the initial findings of the empirical study included in this volume, *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*. This study surveys all fifty states' cybersecurity governance practices and structures to understand what states are doing on the ground, and what works and doesn't.

The final panel of the day focused on government and governance issues in cybersecurity. The panel was moderated by David Thaw (Pittsburgh Law and Information Science), and included Emefa Agawu (New America Foundation), Brian Nussbaum (Albany-SUNY Public Policy & Administration), Charlotte Tschider (Mitchell Hamline; Owner Cybersimple Security), and Tyler White (Nebraska Political Science). In many ways, this panel served as a capstone discussion for the day, tying together themes discussed throughout the day and placing them all in the context of government and governance. Emefa

Agawu and Brian Nussbaum presented aspects of their research into how state and local governments address their own cybersecurity issues, both considering the tensions between the requirements of competent cybersecurity governance and the limitations of state and local government. David Thaw and Tyler White turned an institutionalist eye to these problems, thinking about governance challenges from the perspectives of administrative law and international relations. This led to a fluid discussion of the complex interrelationships that characterize the cybersecurity ecosystem, tying law enforcement, critical infrastructure, government, and private actors together. The highlight of the discussion was surely Brian's anecdote about a local government computer system that had been defaced by attackers: when municipal authorities were contacted, they responded that the system was maintained by a family member who was on vacation, so they wouldn't be able to do anything about it for a week—although a humorous anecdote, it emphasizes that many local and state governments fundamentally lack the resources and expertise needed to address cybersecurity issues.

Professor Thaw and Emefa Agawu both have contributions appearing in this volume. David's Article uses the example of rules and regulations requiring the use of complex passwords—a common but empirically unfounded practice—to explore the challenges of engaging in sound policymaking in technologically-complex settings such as cybersecurity. Too often, he argues, we rely on apocryphia, anecdote, intuition, and other folk wisdom in settings where such heuristics not only do not necessarily provide a basis for good rules but can lead to affirmatively bad rules. Emefa's Article looks at the cybersecurity challenges created by the increasing demands of e-government. Modern government increasingly provides and relies upon Internet-connected services, from using the Internet to provide access to services and information to allowing citizens to pay bills and taxes online and using the Internet internally to coordinate government services. But as governments—and especially local governments—increasingly deploy such services, the challenges to the security of systems on which these services are built—challenges that local government is in a particularly poor position to address—will only rise in importance.

It has been a pleasure working over the past year to bring this conference and symposium to pass. I hope you enjoy and learn as much from the Articles in this volume as I have.