

Symposium Introduction: Swimming in the Ocean of Big Data

Denise C. Bell*

Little could we at the *Journal of National Security Law & Policy* have anticipated in February 2013 how prescient our inaugural symposium would be. Just months after the National Security Agency (NSA) General Counsel, Raj De, presented the keynote speech at “Swimming in the Ocean of Big Data: National Security in an Age of Unlimited Information,” Edward Snowden made international headlines when he divulged top-secret information on, among other topics, the NSA’s Big Data (“metadata”) operations. Thanks to the exceptional gathering of experts in national security, Big Data, and civil liberties who presented at the symposium, anyone who attended the event would have felt comfortable wading through the ocean of revelations made by Snowden. Neither would they have been surprised to learn that Big Data, like in the commercial realm, was just as important in national security.

For those not fortunate enough to attend the *Journal’s* inaugural symposium, the clarity and relevance of the information stands true today. At heart, this issue, like the symposium, focuses on demystifying Big Data and delineating the legal, policy, and normative questions surrounding its use in national security. Readers will find clear, accessible explanations of Big Data and probing conversations considering the tangle of privacy, civil liberties, and national security issues inherent in metadata collection and analytics.

Tackling the challenge of explaining the meaning and mechanics of Big Data, Professor Sean Fahey and Dr. Matthew Gordon lay a technical baseline. Professor Fahey’s discussion of the democratization of Big Data provides historical context for understanding its ubiquity in national security and commercial settings. Dr. Gordon in turn breaks down the pillar components necessary to make successful use of Big Data in any setting: “data integration, search and discovery, knowledge management, and collaboration.” Together, their articles demonstrate how accessible, scalable methods for storage and analysis, combined with a proliferation of sensors, have made Big Data both a potent and problematic tool.

Just as Professor Fahey’s and Dr. Gordon’s articles clarify the opacity of Big Data, they also reveal the fundamental civil liberties and privacy interests implicated in its application, which our other contributors guide us in understanding. In a rare speaking engagement, The Honorable Raj De succinctly lays out the legal framework and policy considerations governing the NSA’s collection and analysis of communications metadata. His final analysis is one with which

* Senior Symposium Editor, *Journal of National Security Law & Policy*, 2012-2013; Georgetown University Law Center, Class of 2013; and Judicial Law Clerk in Executive Office for Immigration Review, Department of Justice. © 2014, Denise Bell.

our readers can agree: not only is Big Data “transforming the world in which the NSA carries out its mission,” meeting the complexities, challenges, and opportunities of Big Data is imperative. How to meet that imperative, of course, animated the symposium and continues to drive debates in a post-Snowden world.

Using two case studies of foreseeable Big Data applications, a roundtable of experts, moderated by Professor Stephen Vladeck, squarely addresses the challenges and opportunities identified by The Honorable Raj De. Presuming that metadata collection will continue apace, the roundtable discussion centers instead on what is considered the more pressing concern: regulating access to and utilization of metadata. As Professor Vladeck discusses in his introduction, concern once centered more on restricting collection in the first place. Perhaps in recognition of Big Data’s utility, focus has shifted to “recalibrating how that data can be used, and by whom.” Indeed, reconciling the utility of Big Data with its ubiquity and potential misuse is a central theme of the symposium. Touching on issues such as primary and secondary use of metadata, data sharing, and the retention of metadata, the roundtable lays a road map for key legal and policy questions we need to address now so that we keep pace with the rapid technological advancements underpinning Big Data. In keeping with this roadmap, the roundtable also notes the urgent need for education and advocacy before lawmakers and policymakers to address Big Data’s contribution to the shrinking space for privacy and Fourth Amendment protections.

While readers will walk away with a better grasp of Big Data, the need remains for a greater structural understanding of Big Data in order to better harness its power and direct its applications for the benefit of national security and protection of civil liberties. Big Data is already a proven, potent tool in the national security – and, indeed, commercial – toolbox. Its utility is such that it is part of the fabric of everyday life. But the task remains in creating a stronger, more nuanced rights- and privacy-protecting legal and policy framework in which to use that tool. The case studies demonstrate that we can predict what future applications of Big Data will look like and the legal and policy questions that will arise. What actions are necessary today to better harness Big Data? As our contributors observe, we are perennially behind in this task, and the urgent takeaway is to act now in concrete ways so that in ten years, we do not find ourselves having the same conversation.

Assembling the group of remarkable speakers and organizing the symposium would not have been possible without the assistance of numerous people, beginning with the speakers themselves. Despite busy and demanding schedules, they were exceptionally generous in their time in participating in the symposium and submitting articles for this issue. Very special thanks goes to the *Journal’s* co-sponsor for this event, the Georgetown Center on National Security and the Law and its Executive Director, Nadia Asanchev. Her guidance kept the event on path and moving forward. The *Journal’s* Board was similarly instrumental in bringing the symposium to fruition. It nurtured a fledgling

journal team and, thanks to its considerable expertise, helped secure a remarkable roster of speakers. Professor Laura Donohue, as faculty advisor to the *Journal*, was indispensable in making the symposium a success.

Special, warm thanks go to Bill Banks, esteemed Professor of Law at Syracuse University and the *Journal's* Editor-in-Chief, who communicated only complete confidence in the symposium team from the very start, and to Carrie Cordero, Director of National Security Studies at Georgetown Law, whose advice and hands-on support were instrumental in making the symposium a resounding success. Both were like mentors. The expertise of Kara Tershel from Georgetown Law's media relations office ensured the symposium generated the media attention it deserved. The National Security Law Society supported and promoted the event at every key step.

Last, but certainly not least, are those who organized the event behind the scenes, including the invaluable, magic-working Kiana Graham from Special Events, Anna Selden and Archie Sridhar from the Office of Journal Administration, Virgil Wheeler from Facilities, and the AV staff who helped us get our technical house in order. Each was generous in their time and patience and always good-humored, despite repeated requests for help and accommodation, and the show, so to speak, went off without a hitch thanks to them.

A final word of thanks goes to the assistant Symposium Editor, Jennifer Logan, whose insight, resourcefulness, and resounding good cheer made organizing the event a pleasure – and the success it was.
