Secrecy and Accountability in a Digital Age

realclearpolitics.com/articles/2014/01/16/secrecy_and_accountability_in_a_digital_age_121248.html

Berkowitz's piece is the first in a series of nine essays to be published by the Hoover Institution over the next week and a half focusing on intelligence gathering in a digital age.

Edward Snowden's theft of massive numbers of National Security Agency (NSA) documents — the Pentagon estimates he copied 1.7 million intelligence files — and the distribution of those documents to journalists who have sporadically published them has damaged American national security interests around the world by delivering to our adversaries sensitive secrets about US intelligence and military operations. The means by which the NSA collects intelligence have been seriously compromised as have been the numerous relationships on which that collection depends, all to the serious detriment of our security.

So far the pilfered documents have not exposed substantial instances of unlawful conduct by the United States government. Nevertheless, much of the public controversy sparked by the revelations about America's extensive electronic surveillance has revolved around allegations of government wrongdoing.

In fact, it was no secret that the United States government, partly in response to the threat of transnational terrorism, has for many years engaged in the collection of enormous amounts of information about telephone calls within the United States, calls between the United States and other countries, and calls entirely outside the United States, and that the government has been mining the data. It had also been reported, though never officially confirmed, that the government was collecting and mining enormous amounts of data concerning email traffic that passes through the United States.

Less well understood are the complex laws, procedures, and oversight mechanisms that the United States has adopted to protect citizens' privacy while culling from its vast pool of digital data only information relevant to the nation's security. To be sure, in an age in which the size, scope, and kind of data are increasing with astonishing speed, those procedures are far from perfect and are in need of regular review and constant refinement. Our constitutional tradition, moreover, teaches the importance of unceasing vigilance whenever the government exercises power, especially when it does so in secret. The vital national security interests served by electronic surveillance do not lessen the concern about the potential abuse of government power.

In this edition of The Briefing, members of the Hoover Institution's Jean Perkins Task Force on National Security and Law deftly explore the complex considerations — technological, legal, political, and strategic — that should inform government's ability to conduct electronic surveillance and keep secrets while protecting citizens' rights and ensuring democratic accountability.

My colleagues provide no easy answers. They do bring into focus the hard issues involved in reconciling the claims of security and of law in a dangerous and digital age.

Berkowitz's piece is the first in a series of nine essays to be published by the Hoover Institution over the next week and a half focusing on intelligence gathering in a digital age.

Peter Berkowitz is the Tad and Dianne Taube senior fellow at the Hoover Institution, Stanford University. His writings are posted at PeterBerkowitz.com and he can be followed on Twitter @BerkowitzPeter.

This article is reprinted with permission from the Hoover Institution.