FROM 9-11 TO JANUARY 6: THE LIMITS OF SURVEILLANCE AUTHORITY AND THE DEMOCRATIC STATE

MARC ROTENBERG*

A Constitutional democracy that seeks to monitor the private lives of its citizens must do so in the most minimally intrusive manner, ensure that its conduct is lawful and permissible, subject to public oversight and transparent, and also that it is effective. Implicit in the willingness of citizens to permit some degree of intrusion by the state is the assurance that the government will act appropriately on the information it obtains. If the government fails to act, it calls into the question the legitimacy of all surveillance authorities.

Others will comment on the extraordinary breakdown in agency coordination and intelligence assessment that made it possible for a mob to seize the Capitol of the United States on January 6, 2021. But a meaningful analysis of January 6 should also take account of the failure of the extraordinary surveillance authorities established after September 11.

After the attack on September 11, 2001, the United States established an extensive system of national surveillance. The telephone records of all Americans were collected in bulk without any suspicion of wrongdoing in the belief that massive data collection would make possible the detection of future terrorist acts. The nation's capital was covered with surveillance cameras. Airline travelers were subjected to x-ray searches at airports that allowed government officials to view the contours of their naked bodies. The Department of Homeland Security monitored journalists and Internet posts, not only for possible threats to public safety, but also for criticisms of the agency. The DHS funded systems such as the Future Attribute Screening Technology to determine "mal- intent" by screening people for psychological and physiological indicators.

The National Security Advisor proposed to link together all public and private databases, and to establish new systems of public surveillance, such as facial recognition, in a vast network called Total Information Awareness. Not far from Washington, DC, a dirigible, part of a multi-billion dollar defense program, floated above the Aberdeen Proving Ground to detect attacks on the Nation's capital by land, sea, and air.

Many of these programs were later found to be ineffective, unnecessary, or simply boondoggles. After several hearings in the Senate Judiciary Committee, and a report from the Privacy and Civil Liberties Oversight Board, Congress repealed the vast surveillance authority created by Section 215 of the Patriot Act. The x-ray imaging devices were replaced by less intrusive millimeter imaging devices. The "Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System" was grounded for good after the dirigible broke free from its tether and floated and crashed into a forest in central Pennsylvania. Reports from the Inspectors General raised questions, still to be resolved, about such surveillance programs as Section 702 of the Patriot Act.

Still, the architecture of surveillance established after 9-11 largely remains in place. And there is more surveillance ahead. Police agencies are deploying body cameras that enable

routine recording of interactions with the public. Predictive policing models allocate resources based on data sets that often contain bias and also seek to establish their own validity. Competition with China in the field of AI provides, for some, an opportunity to argue for relaxation of well-established safeguards in the Privacy Act for personal information in government agencies to create larger data models.

A careful assessment of January 6 should take account of the surveillance programs previously established as well as pending plans to expand data collection. Here are some preliminary recommendations.

1) A full assessment of the events of January 6 should be the starting point. Herb Lin and Amy Zegart, with the Hoover Institution at Stanford University, have set out a comprehensive approach for a Commission on the Capitol Siege that Congress should pursue. As they explain, "[t]he commission's mandate should not be limited to uncovering what happened and making recommendations. It should also be tasked with collecting and preserving information about this unprecedented event for future generations of policymakers, scholars and citizen."

2) A reevaluation of the surveillance techniques established after 9-11, particularly in light of the bias reflected in many of these measures. For example, the Department of Homeland Security obtained otherwise confidential data about Muslim-Americans from the Census Bureau.

3) The incoming Department of Justice should carry forward the 2014 DOJ report on Predictive Analytics in Law Enforcement. That report focused on the limitations of automation in criminal sentencing but also warned that even when algorithms "seem neutral, any model is susceptible to importing any biases reflected in the underlying data." That is a key insight for data driven models of policing.

4) The end of Section 702 of the Patriot Act. The NSA, as well as others, have acknowledged the limited value of this program. To much of the outside world, the ongoing mass surveillance of the communications of non-citizens, while U.S. nationals storm the Capitol, cannot be explained or easily justified.

A broad coalition of civil rights and civil liberties organizations has rightly warned against a new expansion of terrorism-related legal authority after January. There should also be a top-to-bottom review of the surveillance authorities established after 9-11. Lawmakers should proceed cautiously with data driven solutions to public safety challenges. Surveillance without safety may be sufficient for some forms of government, but for democracies it is untenable.

* *Marc Rotenberg is an Adjunct Professor at Georgetown Law and a former Counsel to Senator Patrick Leahy on the Senate Judiciary Committee. He testified before the 9-11 Commission on "Security and Liberty: Protecting Privacy and Privacy Surveillance," and subsequently litigated many cases against the TSA, the DHS, and other federal agencies concerning the use of suspicionless search techniques.*