Time for a Rigorous National Debate About Surveillance; Post-9/11 measures have been weakened or discarded. A coherent new approach is needed.

Pompeo, Mike; Rivkin, David B, Jr. **Wall Street Journal (Online)** [New York, N.Y] 03 Jan 2016: n/a.

Abstract

Forcing terrorists into encrypted channels, however, impedes their operational effectiveness by constraining the amount of data they can send and complicating transmission protocols, a phenomenon known in military parlance as virtual attrition. [...]the use of strong encryption in personal communications may itself be a red flag. [...]the importance of building enduring public support.

Full Text

America is in a long war against a resilient enemy capable of striking the homeland, but U.S. intelligence capabilities are falling short of meeting the threat. The San Bernardino attackers were not flagged, despite their repeated visits to jihadist websites, alarming posts on social media, and suspicious financial transactions. The Boston Marathon bombers evaded timely detection, as did the would-be shooters in Garland, Texas, who had exchanged dozens of messages with a known terrorist overseas.

Paris and San Bernardino exemplify the two types of threats: overseas-trained terrorists, and online-radicalized lone wolves. Both exhibit distinctive behavioral and communications patterns that can be detected--but only if intelligence agencies have the right data and tools to analyze it.

Yet Washington is blunting its **surveillance** powers. Collection of phone metadata under the Patriot Act was banned by Congress and finally ceased at the end of November. Collection of the contents of specific targets' communications under the Foreign Intelligence **Surveillance** Act has been dumbed down, with onerous requirements to secure the authorizing court order. The intelligence community feels beleaguered and bereft of political support. What's needed is a fundamental upgrade to America's **surveillance** capabilities.

Congress should pass a law re-establishing collection of all metadata, and combining it with publicly available financial and lifestyle information into a comprehensive, searchable database. Legal and bureaucratic impediments to **surveillance** should be removed. That includes Presidential Policy Directive-28, which bestows privacy rights on foreigners and imposes burdensome requirements to justify data collection.

There has been much debate about whether providers of communications hardware and software in the U.S. should be obliged to give the government backdoor access. Such a mandate would do little good, since terrorists would simply switch to foreign or home-built encryption. New technologies can cloak messages in background noise, rendering them difficult to detect.

Forcing terrorists into encrypted channels, however, impedes their operational effectiveness by constraining the amount of data they can send and complicating transmission protocols, a phenomenon known in military parlance as virtual attrition. Moreover, the use of strong encryption in personal communications may itself be a red flag.

Still, the U.S. must recognize that encryption is bringing the golden age of technology-driven **surveillance** to a close, which necessitates robust human intelligence. Pursuing every lead on terrorist activity would require a substantial increase in FBI funding and personnel--perhaps double or triple the number of field agents capable of tracking suspects. The Paris attacks, whose perpetrators exchanged numerous unencrypted text messages, were a grim reminder that capable but overstretched security services cannot thwart every terrorist plot.

Congress and the administration should also reassure the intelligence community by reiterating their full support for current **surveillance** programs. Revitalizing cooperation with foreign intelligence partners, which greatly decreased in the wake of Edward Snowden's disclosures, is essential. This would require serious dialogue between world leaders and assurances that security has been tightened to prevent similar leaks.

Enhanced congressional oversight--a true partnership between the executive and Congress--is needed. Each month the intelligence community should provide classified briefings to the House and Senate intelligence committees on how **surveillance** programs are working, what actionable information has been developed, and whether mistakes or abuses have occurred. These briefings should be recorded, and lawmakers should sign an acknowledgment of their attendance. This would bolster accountability and ensure that nobody suffers a memory lapse, such as Nancy Pelosi's failure to remember that she was extensively briefed on the CIA's enhanced-interrogation program.

None of this can happen without a **rigorous** national debate about **surveillance**, launched by congressional hearings. A review of the post-9/11 **surveillance** successes and failures needs to be a prominent part of this discourse. Most disagreements on **surveillance** are about policy, not law: Reasonable warrantless searches are compatible with the Fourth Amendment. So are searches of data shared with third parties, such as social-media posts--a highly valuable **surveillance** window, since people undergoing radicalization are prone to showcase their zealotry online.

In the wake of 9/11, **surveillance** reforms were adopted virtually overnight, with little discussion; they did not last. Hence the importance of building enduring public support. **Surveillance** should feature prominently in the 2016 presidential campaign, giving the next commander in chief a mandate and sense of obligation to implement reforms. Opposition to **surveillance** has been bipartisan, and the strategy for overcoming it must be bipartisan too.

Assertive efforts to defeat Islamic State will diminish, but not eliminate, the threat. Quick response by law enforcement is vital to limiting casualties and neutralizing attackers but cannot entirely prevent terrorism. Even the best 21st-century **surveillance** system won't have a 100% success rate. But robust **surveillance**, drawing on a variety of technical and human intelligence and backed up by **rigorous** investigation of all leads,

is the best way to mitigate the threat.

Mr. Pompeo, a Republican from Kansas, sits on the House Permanent Select Committee on Intelligence. Mr. Rivkin, a constitutional lawyer, dealt with intelligence oversight while serving in the Justice Department and the White House Counsel's Office during the Reagan and George H.W. Bush administrations.

Credit: By Mike Pompeo And David B. Rivkin Jr.

Word count: **837**