National Commission on Terrorists' Use of Technology Is Needed

By Matt A. Mayer

January 2016

- *In an era of ever-changing technology, we must minimize government intrusion while ensuring that law enforcement has the tools necessary to keep Americans safe.*
- *Policymakers have suggested legislation that forces technology companies to alter their software to allow government access to more data. Companies claim this will make it easier to steal data and manipulate the software and will undermine the companies' position in the marketplace, harm shareholder value, and eliminate competition.*
- *Congress and the president should create a commission of experts to analyze issues involved in encryption and provide recommendations on balancing private-sector equities, civil liberties, and national security.*

Over the last year, Americans faced revelations about the National Security Agency's (NSA) telephone metadata collection program, the savage terrorist attack in Paris, and the husband-wife terrorist attack in San Bernardino. Each raised serious questions about the government's use and misuse of data, the effectiveness of data-analysis programs, and law enforcement's technological limits in tracking terrorist activities.

With the 24-hour news cycle and social media outlets, policymakers and pundits are quick to take to the airwaves to show outrage, demand changes, and hold hearings. Rarely do these actions lead to smart government reforms, and in some cases they produce laws that go beyond actions the federal government has historically taken.

There is a real risk policymakers will cross such a line on the issue of encryption.[1] Some have suggested Congress should mandate that private-sector companies create vulnerabilities in their software to allow law enforcement access to encrypted communications. Such a mandate would be unprecedented and a possible overcorrection that does more long-term harm than good. At the same time, the status quo makes law enforcement's job of protecting us nearly impossible. Before Congress acts, a robust debate must occur so policymakers can make the soundest decision possible.

Therefore, a national commission of experts should analyze the issues involved in encryption and provide Congress and the president with recommendations on how best to protect private-sector equities while giving law enforcement the necessary tools to protect us from increasingly sophisticated terrorists.[2] Because both law enforcement and the private sector have legitimate concerns over how best to move

forward on encryption technology, allowing a commission to deliberate on the issue outside of the spotlight of congressional hearings and the prying eyes of our enemies is the safest course of action.

Unlike most think tank reports that contain tidy solutions, this report acknowledges this issue's complexity and the need for expert analysis to fully evaluate the available options. The solution proposed, however, is more than mere process aimed at kicking the can. A properly structured, manned, and directed national commission can give America the best chance of making the least-worst choice.

Let me be clear: if Congress does nothing, we make it easier for terrorists to attack us, because we tie law enforcement's hands once terrorists use encrypted technology to evade them. If Congress requires technology companies to add backdoors to their software, we likely chase consumers, including terrorists, to applications made outside of the United States, undermining our technology industry.

We have been dealt a bad hand that we must play adroitly to win.

The Encryption Challenge for Government

Today, federal agencies and local law enforcement analyze online data to detect potential terrorist threats. In many cases, this analysis consists of reviewing posts on social media, such as Facebook, Twitter, Snapchat, Surespot, WhatsApp, and Telegram. Certain posts are reviewed based on the use of particular words and phrases. Federal agencies and a few large local law-enforcement agencies conduct this analysis in several languages: English, Farsi, Arabic, Urdu, Pashto, Turkish, and Punjabi, to name a few.

If a posting contains enough specificity or the individual posting comments shows a certain level of intensity, analysts will seek other information on that individual. For example, an analyst might investigate where the individual lives (because his location determines the legal jurisdictional lines between federal agencies and local law enforcement), his criminal history, and his links to subjects of ongoing investigations. Once enough information about the individual is gathered, the analyst will discuss the case with supervisors, who then decide whether to seek judicial approval to gather more information.

If Congress does nothing, we make it easier for terrorists to attack us, because we tie law enforcement's hands once terrorists use encrypted technology to evade them.

Once a judge approves, law enforcement orders a technology company to provide information not available from open sources. For example, the company has hard data on location, deleted posts, and other account information. These data allow law enforcement to further build its case that the individual may be engaged in terrorist activities.

A problem arises, however, if the individual moves from a nonencrypted technology application to an encrypted one, which often happens as terrorists' plans become more specific. Law enforcement refers to this movement as "going dark." At this point, law enforcement hits a wall. For example, in a case in Garland, Texas, Elton Simpson exchanged more than 100 messages with jihadists on the day of the attack.[3] Even with judicial approval, law enforcement cannot get additional information from the encrypted technology company because the company itself may not be able to collect any data—the data are encrypted even from them.

With the rise of technology applications, citizens and companies have demanded encryption to keep their conversations, pictures, and other activities shrouded and safe from hackers.[4] This demand stems from a desire to maintain their privacy and, post–Edward Snowden revelations, keep government eyes blocked from their activities. To meet this demand, technology

companies have produced encrypted applications.[5] For example, with the release of iOS8 and higher, Apple has encrypted its telephones without any backdoor that allows it to collect data and, therefore, be responsive to judicially approved government orders.[6]

Yet terrorists are consumers, too. With the NSA revelations by Snowden, terrorists have figured out how intelligence agencies monitor and track them. They now increasingly use encrypted technology to communicate, plot, and attack.

Beyond terrorism, encryption could and likely is being used by transnational organizations and criminals to facilitate human trafficking, drug production and distribution, and other illegal activities. Many Americans may not see terrorism as an imminent threat to them, but most communities face the scourge of drugs and drug-related crimes.

Crossing the Rubicon on Encryption Technology

If terrorists use encrypted technology, we truly have no way to track them other than with human intelligence, which is incredibly expensive, labor-intensive, and high risk for the undercover agents. As Americans, we must soberly ask ourselves if we are willing to live in an environment where law enforcement is unable to protect us.

In fact, shortly after the San Bernardino attack, Federal Bureau of Investigation Director James Comey briefed policymakers. While investigators "wouldn't say that San Bernardino suspects Syed Farook and his wife Tashfeen Malik used encrypted communication to avoid detection, they said it could have been used and that it is becoming an increasingly big impediment that prevents investigators from collecting information about either co-conspirators or future attacks."[7]

Daesh and other terrorist groups are sophisticated users of technology. In fact, leveraging technology has become a core terrorist capability. Whether creating slick recruiting videos or distributing jihadi material across multiple technology channels, terrorists, like ordinary consumers, identify and use the most secure and reliable applications to do their work. Before encryption, law enforcement could keep a close eye on suspected terrorists and harness judicial resources to expand its investigations.

When terrorists go dark with encrypted technology, law enforcement loses its ability entirely to track terrorist communications. It is possible to leverage other avenues, such as tracking financial movements and travel, to gain at least some knowledge on a particular terrorist. If, however, terrorists go dark in the final phase of an attack and communicate execution orders via encrypted applications, law enforcement's ability to detect, disrupt, and prevent the attack becomes a matter of pure luck.

A chorus has arisen in Washington, DC, to pass legislation forcing technology companies to insert "backdoors" into their software to allow government agencies to access data currently unavailable to them. Technology companies claim that creating backdoors will make it easier for hackers and rogue regimes to steal data and manipulate the software for bad purposes.

Equally important, technology companies state that their encryption technology is a competitive advantage that goes to the core of their offerings to private citizens (and three-letter government agencies). Legislation forcing them to create backdoors would undermine their position in the marketplace, harm shareholder value, and eliminate competition. Director Comey, along with Senate Intelligence Committee Chairman Richard Burr (R-NC), suggested that "technology companies might need to consider changes to their 'business model.'"[8]

Whether or not these claims are completely accurate, they make a fundamentally important point: legislators will force private-sector entities to take specific actions related to their products that are contrary to what executives believe is right for their companies. Legislators are placing themselves de facto on the boards of directors for privately and publicly traded companies. This action is unlike regulatory or compliance legislation that prohibits certain actions deemed improper, illegal, or harmful to consumers who use the product.

Consumers are not harmed by using Twitter or Snapchat without a backdoor. In fact, the lack of a backdoor keeps consumers safer from hackers. To the contrary, such legislation will likely harm consumers because it will limit their choices when companies either comply with the law, thereby making their product less attractive to consumers, or choose to exit the US market to avoid the law. By using encrypted applications, consumers have expressly stated their preference for encrypted technology. Similarly, if the legislation forces some technology companies out of the market, it could lead to higher prices.

As with water flowing downhill, the private sector will go where it can do business with the highest level of certainty, legal protection, and beneficial tax law.

Moreover, instead of enhancing our ability to detect terrorists, legislation could reduce it. Specifically, legislation could result in consumers and terrorists using encrypted applications developed and released in foreign countries. Once Congress passes backdoor legislation, the US will lose its current influence to work quietly with technology companies and arrive at a potential win-win solution.

It must be the government's position that, because software does not have a backdoor, the government cannot track terrorists, and therefore citizens' safety is at risk in a very general sense (that is, from a future terrorist attack somewhere). There really is no precedent for passing legislation that forces a private-sector company to do something to its technology that was contrary to what it deemed best. The USA Freedom Act of 2015 required telecommunication companies to store data, which imposed a cost on those companies.[9] That requirement, however, did not attack the business model or competitiveness of those companies. It also did not force companies to alter their products.

Finally, encryption legislation could quash the technology advantage America has built over the last 40 years. After all, if technology companies now need to fear coercive government meddling in their product development, those companies may seek other jurisdictions where certainty from government action is higher.

For example, Switzerland's strong privacy laws in banking have for years made it a safe place to store assets. Similarly, Delaware's strong corporate laws compared with the laws of other states made it the primary jurisdiction for corporations to establish their principal place of business. Pfizer and Allergan's recent merger for tax benefits in Ireland is another example in which companies will act to strengthen their positions. As with water flowing downhill, the private sector will go where it can do business with the highest level of certainty, legal protection, and beneficial tax law.

Americans Are Right to Fear Big Government

The issue of encryption goes far beyond the debate over the NSA's telephone spying program, which enlivened the Republican presidential debate in Cleveland, Ohio, when US Senator Rand Paul and New Jersey Governor Chris Christie sparred over it.[10] That said, Americans are generally concerned with the government's access to and use of personal records.

As the United States Court of Appeals for the Second Circuit held in finding the NSA program illegal:

> Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. *But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language*.[11] (emphasis added)

A man does not have to wear a tinfoil hat at home or believe Big Brother is constantly monitoring his car to have legitimate concerns about government invasions of private life. Unlike the NSA program that involved only metadata, preventing encryption renders all communications potentially discoverable, including actual conversations.

If the outcome of this debate is that technology companies must provide the government with a database of all communications, Americans should have little faith that those communications will be protected. As the US Government Accountability Office (GAO) found:

> Inspectors general at 22 of the 24 agencies cited information security as a major management challenge for their agency. For fiscal year 2014, most of the agencies had information security weaknesses in . . . limiting, preventing, and detecting inappropriate access to computer resources. . . .
>
> The federal government continues to face challenges in effectively addressing increasing concerns about the protection of the privacy of personally identifiable information (PII). The number of reported security incidents involving PII at federal agencies has increased in recent years, rising from 10,481 incidents in 2009 to 27,624 incidents in 2014.[12]

Americans read about data breaches of federal computers too often not to be concerned with what the federal government is collecting and how it is safeguarding that data.

Beyond collecting data directly from citizens when they pay taxes or apply for benefits, government entities also purchase data from private-sector resellers. This raises an additional concern for citizens: namely, how government employees and contractors use the data they collect. GAO found that "some agencies lacked robust audit mechanisms to ensure that use of personal information from information resellers was for permissible purposes."[13] In fact, GAO noted that "components with each of the four agencies did not consistently hold staff accountable by monitoring usage of personal information from information resellers and ensuring that it was appropriate."[14]

Government must do a far better job of protecting personal data, limiting access, and ensuring the data are used for proper purposes. Citizens' adoption of encrypted technology is a direct response to the problems already noted, as well as a general desire to maintain their privacy. As noted earlier, however, encryption will make it more difficult for law enforcement to detect and stop terrorist attacks.

Commission Purpose, Membership, and Duration

Before Congress acts, the wisest and safest course of action for America is patience and investigation to ensure that we balance law enforcement's need for data against the private sector's right to rise or fall in the marketplace without government interference. Congress should create a commission to dig into this issue thoroughly and quickly, and the commission should release its recommendations before Congress enacts any legislation that directs private-sector companies to act.[15]

As with the incredible work done by the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), a commission on terrorists' use of technology would have the power to:

- Hire and consult with the required staff and experts to understand the challenges faced by both government and the private sector;
- Review the government's classified and unclassified actions, successes, and failures to date;
- Meet with government and private-sector representatives to understand their concerns;
- Gain access to the core technology of private-sector companies; and
- Identify where the technology is headed and any future issues, including how government can improve its data-protection capabilities.[16]

The goal for the commission is to develop recommendations for Congress and the president that identify how best to protect America without weakening our technology sector. At a minimum, the commission must resolve the dilemma we face in a manner that balances the various equities, knowing that there is not a "right" answer.

Americans have grown skeptical of government, and our faith that government will keep us safe is plummeting.

Every option, unfortunately, brings consequences with which we must be willing to live. Confidence in that resting point will come only if the method by which we got there was thoughtful and vigorous. We are constantly told that the government needs access to more and more data to keep us safe. The commission can review the record to ensure that this claim is accurate and that access to encrypted data is in fact necessary.

A commission of experts focused solely on this issue could accomplish far more than Congress can, especially because members divide their time among committees, fundraising, constituent services, and reelection. Moreover, given the sensitivity of the issue and the trade secrets involved, a commission stands a better chance of securing the private sector's true participation. Finally, while it is impossible to remove politics from a politically created entity, a commission with the right people can rise above politics to provide Congress and the president with the soundest advice possible on an issue that will continue to challenge us for years, if not decades, to come.

The commission would also demystify the issue for Americans, thereby providing us with a greater sense that our government is advancing carefully and is fully aware of the awesome power it holds. Americans have grown skeptical of government, and our faith that government will keep us safe is plummeting.[17] By taking a thoughtful approach to this issue, policymakers can demonstrate to Americans that they can do more than grandstand and demagogue opponents.[18]

Membership on the commission must be both bipartisan and representative of the various interests engaged in this issue. Similar to the 9/11 Commission, it could be comprised of 10 members: two appointed by Republicans, two appointed by Democrats, one appointed by the president, four from the technology sector and jointly appointed by Congress, and one from a civil liberties group and jointly appointed by Congress. The type of members for consideration should include individuals with experience in intelligence and in technology.

Because time is of the essence, the commission should have six months to form, investigate the issue, and issue its recommendations. It is a short timeframe, but this issue must be solved. Failure to do so would weaken our security and create uncertainty in the private sector.

The Balance between Security and Liberty

America has citizens who believe fervently in protecting our civil liberties at all costs and citizens who are willing to give up some civil liberties to increase our security. Throughout American history, a pendulum has swung between the two poles depending on circumstances.

In times of war, the pendulum swung away from civil liberties toward security. When the heat of war faded, citizens forced the pendulum back toward civil liberties. We have also grown as a country, so actions deemed proper in the past are shocking today.

For example, the internment of Japanese Americans in camps during World War II, approved by the US Supreme Court, is an action we look back on with rightful shame.[19] More recently, the use of enhanced interrogation techniques against terrorists has generated enormous and sometimes very heated exchanges.[20]

With encryption, we have the opportunity to dig into the issue to determine as best we can where the pendulum should rest. It is vital we take advantage of this opportunity to minimize government intrusion into core private-sector market strategy and decision making. At the same time, it is paramount that the men and women charged with keeping us safe have the necessary tools to do so.

We are facing thorny questions that go to the core of our liberal democracy. Let's make sure our answers are the right ones—or as close to the right ones as thoughtful deliberation and wisdom allow. A commission gives us the best chance to do so.

About the Author

Matt A. Mayer is a visiting fellow in homeland security studies at AEI. He is a former senior official at the US Department of Homeland Security and the author of *Homeland Security and Federalism: Protecting America from Outside the Beltway* (Praeger, 2009).

Notes

1. Damian Paletta, "Silicon Valley Faces Showdown as Lawmakers Fume over Encryption," *Wall Street Journal*, December 10, 2015, http://blogs.wsj.com/washwire/2015/12/10/silicon-valley-faces-showdown-as-lawmakers-fume-over-encryption/.

2. On December 27, 2015, Representative Michael McCaul (R-TX), chairman of the House Homeland Security Committee, and Senator Mark Warner (D-VA), a member of the Senate's Banking, Finance, and Intelligence Committees, made a similar recommendation in an op-ed in *The Washington Post*. See Michael McCaul and Mark Warner, "How to Unite Privacy and Security—Before the Next Terrorist Attack," *Washington Post*, December 27, 2015, https://www.washingtonpost.com/opinions/how-to-unite-privacy-and-security--before-the-next-terrorist-attack/2015/12/27/628537c4-a9b3-11e5-9b92-dea7cd4b1a4d_story.html.

3. Evan Perez, Pamela Brown, and Jim Sciutto, "Texas Attacker Had Private Conversations with Known Terrorists," CNN, May 7, 2015, http://www.cnn.com/2015/05/07/politics/fbi-warning-elton-simpson-cartoon-event-attack/.

4. Devlin Barrett, "FBI Seeks to Reframe Encryption Debate," *Wall Street Journal*, December 30, 2015, http://www.wsj.com/articles/fbi-seeks-to-reframe-encryption-debate-1451417252.

5. Paletta, "Silicon Valley Faces Showdown."

6. Again, this goes beyond Sen. Paul's requirement for law enforcement to just get a search warrant.

7. Paletta, "Silicon Valley Faces Showdown."

8. Ibid.

9. USA Freedom Act of 2015, P.L. 114-23, June 2, 2015, https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf.

10. Fox News, "Chris Christie, Rand Paul Spar over NSA," August 6, 2015, http://video.foxnews.com/v/4404624763001/chris-christie-rand-paul-spar-over-nsa/?#sp=show-clips.

11. ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

12. US Government Accountability Office, *High-Risk Series: An Update*, February 2015, http://www.gao.gov/assets/670/668415.pdf.

13. US Government Accountability Office, Testimony before the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform, "Privacy: Government Use of Data from Information Resellers Could Include Better Protections," March 11, 2008, http://www.gao.gov/assets/120/119298.pdf.

14. Ibid.

15. Though I am as wary of federal commissions as anyone, I do think a properly structured and manned commission is the right course of action in this case. If Congress takes up this idea, it should ensure that the commission is structured more like the 9/11 Commission than the countless "blue ribbon" commissions that have looked at entitlement reform.

16. "National Commission on Terrorist Attacks Upon the United States," http://www.9-11commission.gov/.

17. Gallup, "Trust in Government," September 2015, http://www.gallup.com/poll/5392/trust-government.aspx; and Gallup, "Trust in Government to Protect against Terrorism at New Low," December 11, 2015, http://www.gallup.com/poll/187622/trust-government-protect-against-terrorism-new-low.aspx.

18. A careful approach is all the more important given that we are in the midst of a presidential election where emotions run hot and soundbites can drive policy.

19. Korematsu v. United States, 323 US 214 (1944).

20. Brian Ross and Richard Esposito, "CIA's Harsh Interrogation Techniques Described," ABC News, November 18, 2005, http://abcnews.go.com/Blotter/Investigation/story?id=1322866.