WILMERHALE

DOJ Tells Tech Companies to Develop "Responsible Encryption"

DECEMBER 5, 2018

On November 29, 2018, in a speech at the Georgetown University Law School, Deputy Attorney General Rod Rosenstein renewed his call for tech companies to build into their products the means for law enforcement to legally access decrypted data, the development of so-called "responsible encryption."[1] Mr. Rosenstein analogized such encryption to requirements that buildings disable elevators in the event of a fire but still retain firemen's access, and he beseeched the private sector to work with the government to mitigate the security threats posed by rapid technological advances.

Summary of Mr. Rosenstein's Address

Detailing the threat of ransomware, Mr. Rosenstein warned that the "malicious use of technology will be more pernicious and pervasive tomorrow than it is today, and even more difficult to combat." To "forestall those ominous consequences," he proposed three steps:

First, technology must be designed such that security is equally considered along with novelty and convenience, in the same way that cars are designed with airbags and ships with floatation devices.

Second, the private sector must work cooperatively with law enforcement agencies on emerging security issues.

Third, because thwarting technologically enabled destructive activities is a "moral imperative," a "culture in which technology companies work to defeat legitimate law enforcement activities" cannot be permitted.

Mr. Rosenstein rejected an argument that tech companies' innovation automatically contributes to the public good. He did not blame the tech companies for "failing to consider" the law enforcement and public safety concerns implicated by their products, but asserted that their profit motive does not require them to anticipate or prevent the misuse of the products they are racing to get to market. Indeed, he described a "fundamental misalignment of economic incentives and security," exemplified by how developing more secure devices requires additional testing and validation, thereby slowing production times.

Rosenstein argued that because of this misalignment between companies' desires to achieve

competitive advantages and public safety, law enforcement's focus on improving cybersecurity, thwarting cyber threats, and improving security across the private and public sectors becomes all the more important. Law enforcement must be able to identify perpetrators and impose punishment. The private sector, Mr. Rosenstein asserted, should not hinder that effort. He called out communications providers for understaffing their offices that respond to law enforcement requests and complained about so-called "warrant-proof" encryption, whereby products are designed in such a way that it is impossible for tech companies to assist in executing warrants. Instead, Mr. Rosenstein encouraged tech companies to develop responsible encryption—"effective, secure encryption that resists criminal intrusion but allows lawful access with judicial authorization."

Mr. Rosenstein took the position that security researchers, technology companies, academics and information security professionals refusing to help develop responsible encryption is not "virtuous." Instead, tech companies "share a duty to comply with the law and to support public safety, not just user privacy." Ultimately, the collaborative search for security solutions "will enable us to harness the wonder of new advances without descending into technological anarchy."

Key Takeaways from Mr. Rosenstein's Address

Technology companies should take away several key points from Mr. Rosenstein's speech.

First, the speech suggests that the Trump administration will take a hard line against the tech industry's trend toward unbreakable encryption. This is not Mr. Rosenstein's first time calling for responsible encryption, and it will likely not be his last. In fact, in an August 30, 2017, speech, Mr. Rosenstein lamented tech companies' alleged unwillingness to help enforce court orders to obtain evidence stored on electronic devices,[2] and in an October 10, 2017, speech, Mr. Rosenstein specifically described a need for responsible encryption.[3] And Mr. Rosenstein's calls will likely continue despite evidence that the FBI has repeatedly provided inflated statistics to Congress and the public about the extent of problems posed by encrypted cellphones.[4]

Second, Mr. Rosenstein's speech may signal the federal government's increasing willingness to litigate disputes with tech companies that refuse to voluntarily cooperate with law enforcement to produce decrypted information.

Third, the fact that Mr. Rosenstein provided few specifics as to how responsible encryption would actually work may reveal Mr. Rosenstein's belief that the innovation onus lies on the private sector. Indeed, the only details Mr. Rosenstein provided regarding functionality were that any backup key "does not need to be held by a single entity, and it does not need to be held by the government." Mr. Rosenstein's praise in his speech for Ray Ozzie, a former Microsoft executive, who, by his own initiative, "reportedly developed a system that he believes could allow law enforcement access to encrypted data without significantly increasing security risks for users," reinforces an apparent belief that security ingenuity should not be dependent on government funding.

Finally, in encouraging tech companies to design responsible encryption, the Department of Justice is unlikely to be sympathetic to American companies' concerns that including such encryption in their products will reduce their global competitiveness. Foreign businesses, governments and individuals could be wary of devices and messaging challenges that are accessible to the US

government, and demand for American products could decrease globally.[5] Ultimately, the alleged misalignment Mr. Rosenstein describes between market forces and public security may in fact become aggravated by Mr. Rosenstein's persistent call for responsible encryption.

---

1. Rod J. Rosenstein, Deputy Attorney General, Keynote Address at the Georgetown University Law Center's Cybercrime 2020 Conference (Nov. 29, 2018).

2. Rod J. Rosenstein, Deputy Attorney General, Remarks at the 10th Annual Utah National Security and Anti-Terrorism Conference (Aug. 30, 2017).

3. Rod J. Rosenstein, Deputy Attorney General, Remarks on Encryption at the United States Naval Academy (Oct. 10, 2017).

4. *See* Devlin Barret, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST., May 22, 2018.

5. *See* Rina Pfefferkorn, "The Risks of 'Responsible Encryption'" at 9, Feb. 2018, THE CENTER FOR INTERNET AND SOCIETY.

Contributors

Michael Mugmon

PARTNER

Partner-in-Charge, San Francisco Office

michael.mugmon@wilmerhale.com

+1 628 235 1006