Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection Yong Pung How School Of Law

Yong Pung How School of Law

2-2016

Security and privacy must not be traded off against each other

Tan K. B. EUGENE
Singapore Management University, eugene@smu.edu.sg

Follow this and additional works at: https://ink.library.smu.edu.sg/sol_research

 Part of the Privacy Law Commons, and the Securities Law Commons

Citation

EUGENE, Tan K. B.. Security and privacy must not be traded off against each other. (2016). *Today*. 1-4.
Available at: https://ink.library.smu.edu.sg/sol_research/3872

This News Article is brought to you for free and open access by the Yong Pung How School of Law at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection Yong Pung How School Of Law by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

Security and privacy must not be traded off against each other

BY

EUGENE K B TAN

February 26, 2016

Last week, a United States federal judge ordered Apple to assist the Federal Bureau of Investigation to gain entry into an encrypted iPhone used by Syed Rizwan Farook to know where Farook and his wife had been and who had helped them in their terrorist act last December. Farook and his wife shot and killed 14 people in San Bernardino, California, before the police killed them.

Apple is mounting a robust challenge to resist the order arguing that the US government's demands undermine the very freedoms and liberty the government is duty-bound to protect. The implications of (non-)access to encrypted data will be closely watched and studied.

In the midst of this stand-off, the Wall Street Journal reported this week that the US Justice Department is seeking court orders that would compel Apple to help it bypass the security features on at least 12 other iPhones not connected to terrorism cases.

The issue of security versus privacy is one that is occurring more frequently as concerns with terrorism grow. With the increasing use of encryption technology in many electronic devices, law enforcement agencies will likely seek ways and means to access such information.

If a similar terrorist incident happened here, would the Singapore Government also do the same thing? Very likely. The authorities here or elsewhere would seek to have all the available information they believe would be helpful.

As there is no constitutional right to privacy in Singapore, it is much harder, though not impossible, for a company such as Apple to mount a successful legal challenge, on the basis of protection of privacy rights, to such an executive or court order. Nonetheless, questions remain as to whether a person in Singapore is entitled to reasonable expectations of privacy.

Various Singaporean legislations provide the law enforcement agencies here with a broad spectrum of powers to acquire information or to require countermeasures. For instance, Section 40 of the Criminal Procedure Code provides the authorities with the power to access decryption information (coded information made intelligible).

Section 15A of the Computer Misuse and Cybersecurity Act empowers the minister to authorise or direct any person or organisation to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore.

However, Section 58 of the Telecommunications Act seemingly provides a lower threshold for the minister to give directions to a telecommunications licensee, where it is "requisite or expedient to do so", "on the occurrence of any public emergency, in the public interest or in the interests of public security, national defence, or relations with the government of another country".

PROTECTING PRIVACY

Notwithstanding the authorities' broad scope of legislative powers, our courts are likely to defer to the executive on what measures are needed to address security threats on the basis of institutional competence (courts do not have expertise in security matters) and institutional design (the Government is answerable to the people on security matters).

Nevertheless, it is crucial that privacy concerns are given due consideration and weight. They fundamentally affect the trust between a government and its people. The authorities must endeavour to act in a proportionate manner. In this regard, "helpful" information is probably too low a threshold for intrusive action.

To balance the interests of security and privacy, the better and more rigorous standard is whether the information was necessary for a successful prosecution or to deal with a clear and present danger.

For instance, are there alternative sources of information that would suffice? This is, of course, a more demanding hurdle for the authorities to surmount. But it helps ensure that the Government does not overreach and seeks to maintain that delicate balance between security and privacy.

With increased encryption use and its growing sophistication, it is likely that helpful information sought by the authorities for intelligence, investigation and

enforcement measures may not be so easily available to them. In response, law enforcement agencies globally will up the ante in making the case for more access to encrypted data in the interest of national security.

Encryption technology should not be used maliciously or become a dark space for terrorist groups to inflict harm on society. By the same token, governments must not use surveillance tools to arbitrarily target individuals under their protection.

While privacy and security are often presented as necessary trade-offs, the better approach is not to treat them as a zero-sum proposition. Security will be compromised if privacy is given short shrift. Safeguards must be put in place to ensure that any intrusion to privacy, even where legally sanctioned, is sensitively calibrated and proportionate to the threat. Necessity and proportionality must be the hallmarks.

The societal costs of encryption use and mass surveillance and the inadequacy of privacy protection need to be factored in and given due consideration. Ultimately, it is for each society to decide where the balance ought to lie.

Although the fight against terrorism is often offered as an overriding justification for privacy intrusions, this could easily become the slippery slope that paves the way for a situation of exception becoming the norm, undermining the rule of law. The conversation about privacy in the encrypted digital realm in an age of mass electronic surveillance requires the collective expertise and cooperation of governments, civil society and industry to arrive at a viable framework that delicately balances the rights, responsibilities and interests of various stakeholders.

Fighting crime and terrorism cannot be about the authorities using the full suite of powers that the law affords them. Their challenge is also to ensure that citizens' rights and legitimate expectations to privacy are adequately protected, while also steadfastly protecting them from terrorist and criminal activity. Any use of draconian powers must remain alive to the imperative to maintain trust and confidence with the population, and keep faith with the values that are fundamental to what a society stands for.

ABOUT THE AUTHOR:

Eugene KB Tan is associate professor of law at the School of Law, Singapore Management University.