Embargoed until 6am, Thursday, 12 December 2019

MEDIA RELEASE
12 December 2019
Joint media release: University of Waikato and New Zealand Law Foundation

Government's power to order decryption should respect the privacy and rights of users and companies

The power of government to order users and companies to decrypt encrypted data and devices needs stronger privacy protections and additional safeguards, according to a study published by researchers at the University of Waikato.

Encryption is a process of scrambling information to protect it against unauthorised access, alteration or distribution. This technology helps ensure the confidentiality, integrity and authenticity of data and communications. The security and privacy of internet banking, online shopping, cloud services, data storage, secure messaging and many other products and services depend on encryption.

Under the Search and Surveillance Act 2012, law enforcement officers have the power to search and seize encrypted data and computers. This includes the authority to compel users and providers to give up their passwords and access information such as encryption keys. In addition, companies can be required to provide reasonable assistance to allow law enforcement officers to gain access to encrypted data, services and devices. Moreover, under the Telecommunications (Interception Capability and Security) Act 2013, network operators and service providers have a duty to offer reasonable assistance to intercept and collect communications. NZ Customs also has the power to demand passwords and order the decryption of smartphones and other electronic devices as part of customs and border searches.

According to principal investigator Dr Michael Dizon, the problem with these powers is that there are no express standards and guidelines with respect to how they are carried out, especially in relation to human rights. Forcing suspects to disclose their passwords may infringe their right against self-incrimination. Requiring a company to create backdoors or vulnerabilities in encryption to allow the police access to a suspect's data may jeopardise the privacy and security of all its other clients.

"The law does not explicitly say what reasonable and necessary assistance means. There is a potential then for misinterpretation, misapplication and possible misuse of these powers," Dr Dizon says. This is the same dilemma faced in the *Apple v FBI* case where the US law enforcement agency wanted a court to order Apple to create modified software to allow the FBI to gain access to a shooter's locked iPhone. In this case, Apple refused to comply on the grounds that the order was unreasonable, and it would endanger the privacy and security of all its users. However, the FBI found a work around and was able to unlock the iPhone through a technical solution provided by another company.

Findings from focus group interviews conducted by the researchers that involved members of the general public, business and government indicated people in this country place the greatest importance on privacy, data protection and information security when using encryption. Based on these findings, the lack of clear legal and regulatory guidelines in the use of powers exercised by authorities is all the more worrying. Dr Dizon says, "New Zealanders primarily use encryption to protect their privacy and security. Forcing people to disclose their passwords or to render assistance may violate their rights and interests."

The researchers recommend that the right or privilege against self-incrimination should be more strongly recognised in computer searches, and that persons suspected or charged with a crime should not be forced to disclose their passwords. While providers have a responsibility to assist the police in search or surveillance operations if it is within their existing technical capabilities, such assistance should not involve any act that would undermine the information security of their products and services or compromise the privacy of their clients as a whole.

The principal investigators of the study are Dr Michael Dizon, Associate Professor Wayne Rumbles and Prof Ryan Ko. The research report is entitled *A matter of security, privacy and trust: A study of the principles and values of encryption in New Zealand* and is available at https://www.lawfoundation.org.nz/?page_id=6886 or https://www.waikato.ac.nz/law/research/information-law-and-policy-project.

The study received funding from both from the University of Waikato and the New Zealand Law Foundation's Information Law and Policy Project (ILAPP). ILAPP was established to explore and develop law and policy around IT, Data, Information, Artificial Intelligence and cyber issues, as well as to help build New Zealand's digital capability and preparedness.

END

Contact details:
Dr Michael Dizon
07-838-4466 ext 8590
Email: michael.dizon@waikato.ac.nz