STATES OF JERSEY

DRAFT CYBERCRIME (JERSEY) LAW 201- (P.134/2018): COMMENTS

Presented to the States on 28th January 2019
by the Education and Home Affairs Scrutiny Panel

STATES GREFFE

COMMENTS

Introduction

1. The Draft Cybercrime (Jersey) Law 201- (hereafter "the draft Law") is focused on bringing Jersey up-to-date in its treatment of crimes relating to computers and data storage. As drafted, the draft Law would make amendments to the following existing Laws –

   - Computer Misuse (Jersey) Law 1995
   - Criminal Justice (International Co-operation) (Jersey) Law 2001
   - Police Procedures and Criminal Evidence (Jersey) Law 2003
   - Regulation of Investigatory Powers (Jersey) Law 2005

2. If the draft Law is adopted, then Jersey would be in a position to have the Council of Europe Convention on Cybercrime (the Budapest Convention) extended to it. The Convention is concerned with crimes committed over the internet, particularly infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. Further information on the purpose of the Budapest Convention can be found here.

Amendments and contents of the draft Law

3. The amendments to the existing Laws made by this draft Law would be as follows –

   (a) **Computer Misuse (Jersey) Law 1995** – this amendment would update the definitions and penalties for unauthorised access to computer material (hacking), unauthorised modification of computer material (e.g. damaging a computer to hinder access to incriminating data), and also make it an offence to supply or obtain any software or hardware for the purposes of committing a crime online.

   (b) **Criminal Justice (International Co-operation) (Jersey) Law 2001** – this amendment would allow for a preservation order to be granted in the event that the Island was working with another jurisdiction to investigate a crime. This is in order to prevent a suspected party of deleting or destroying data when under investigation. It would also make it an offence to delete or destroy any data that was the subject of a preservation order.

   (c) **Police Procedures and Criminal Evidence (Jersey) Law 2003** – this amendment would allow police officers, subject to an application and permission from the Bailiff, to gain access to any material stored on a computer or on a "cloud based" storage programme.

(d) **Regulation of Investigatory Powers (Jersey) Law 2005** – this amendment would make it an offence for a service provider (i.e. telecoms provider) to tip off a service user about any request from a public authority to investigate any information they may hold. It would also enable law enforcement to require a person to grant them access to a device which is otherwise locked (i.e. mobile phone, tablet, etc.), subject to permission from the Bailiff. Such notice could only be given on the grounds of national security, for the prevention and detection of crime, in the economic interests of Jersey, or to perform a statutory power or duty.

4. The Education and Home Affairs Scrutiny Panel (hereafter "the Panel") wrote to organisations working within the field of cyber security and stakeholders that may be affected in order to gather views on, and identify, any concerns in respect of the draft Law. The Panel received six submissions that commented on the contents and intended actions arising from the draft Law. In order to clarify the concerns arising from the submissions, the Panel raised several questions with the Minister for Home Affairs, the answers to which can be found in the attached **Appendix**. The Panel is satisfied that the answers given have addressed the concerns.

5. The Panel is generally supportive of the draft Law, and is of the opinion that it will create a futureproofed framework to better assist Jersey when dealing with cyber-related crimes. It is also worth noting that the consequences of not adopting this draft Law could be far-reaching. As technology continues to be integrated into society at both a personal and business level, it is vital that protections are in place to guard against the criminal activity that will likely increase alongside it.

6. Whilst the draft Law itself does not require any further amendments at this stage, the Panel would like to raise 2 particular points that should be considered further if it is adopted by the States Assembly.

Engagement with local industry

7. During the course of its review, the Panel was presented with commercially sensitive information which highlighted concern about the implementation and expectation on local industry in respect of the changes being brought forward by the draft Law.

8. The Panel understands that at present a Technical Advisory Board ("TAB") meets on an annual basis with local telecommunications firms, in order to explore any technical and commercial changes that may affect the application and enforcement of the Regulation of Investigatory Powers (Jersey) Law 2005 ("RIPL"). This Board should also look at engaging with other local business and IT service providers where possible if the draft Law is implemented.

9. Whilst there is uncertainty over the potential impact of the draft Law on local industry, the Panel recommends that the TAB meets on a regular basis with representatives of the industry in order to clarify expectations, as well as develop and introduce updated codes of practice governing the draft Law. If the draft Law is adopted by the States Assembly, then the TAB should meet

regularly over the first 6 months to a year after its introduction, to ensure that these concerns are addressed and the draft Law is implemented correctly.

Changes in the world of technology

10. The pace at which technology advances in the modern world continues to accelerate, and with this it is vital that legislatures are cognisant of the changes in terminology and nomenclature in respect of cyber security and offences that can be committed.

11. One particular area that is changing rapidly is in relation to the "Internet of Things". The Internet of things is defined as –

> "*… the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems".*[1]

12. This relates to a myriad of home devices (i.e. smart kettles, Amazon Alexa, etc.) that could, under the draft Law, be used to commit offences. The Panel has questioned how the draft Law would futureproof against this ever-changing area, and received the following response from the Department for Justice and Home Affairs –

> "*In respect of the 'Internet of Things', as per question 8, the two safeguards are a) the current definition of "computer", which is wide enough to capture any data storage device, and b) the capacity of the Courts to interpret 'computer' as needed. If a 'Thing' has sufficient capacity to be Wi-Fi enabled it is likely to be a 'computer' under the Law, and if it is not it must be controlled by something that is a 'computer'. Accordingly, unauthorised access to, for instance, an internet-enabled refrigerator will, prima facie, be a crime under the Law.*"[2]

13. The draft Law does have capacity to understand and react to these changes; however, it must not be seen as the final piece of the puzzle for dealing with cyber-related crime. Constant review of the effectiveness and suitability of the draft Law is vital to ensure that it is reacting to the changes and challenges presented by new and improved technology. The Panel will continue to monitor the implementation of the draft Law and hold the Minister to account.

Conclusion

14. As stated above, the Panel is generally supportive of the draft Law and agrees that, should it be adopted by the States Assembly, it will assist Jersey in the policing and prosecution of cyber-related offences.

[1] https://www.webopedia.com/TERM/I/internet_of_things.html
[2] Questions on the Draft Cybercrime (Jersey) Law 201-

15. The Panel has recommended that consideration is given as to how industry is engaged to understand the changes from the draft Law, and that the Technical Advisory Board meets regularly in the initial stages of its implementation to confirm expectations and develop agreed codes of practice. Likewise, the draft Law should be kept under constant review to ensure that it is reacting to the changes and challenges of the fast-moving world of technology.

16. The Panel will therefore be supporting the draft Law, and will continue to hold the Minister for Home Affairs to account for its implementation.

APPENDIX

Questions on the Draft Cybercrime (Jersey) Law 201- ("the Law")

1. Article 19 – How is "in a timely manner" defined? What is the proposed timescale?

The phrase 'timely manner' is a standard in legislation where the precise timings of the required action depend on the facts and circumstances of the case. Courts have a wide discretion in interpreting this phrase and will seek to do so fairly.

2. Page 20, Section 5D(4) – To what level can a company disclose a request for information to others within the company for the purposes of complying with the request?

If a request has been made to the company itself, then disclosure to individuals within that company would seem to be within the terms of the request, and so should not be an issue.

3. Page 21, Section 3(2)1(A)–(C) – Does this refer to cloud services and or cloud storage?

Yes.

4. Article 5A(i) – What consideration has been given to tools that may be "dual use"? (i.e. can be used for both legitimate and illegal purposes)

The focus of Article 5A(1) is a person's intention that, in making, adapting, supplying or offering the relevant article, it will be used to commit or assist in the commission of an offence under Article 2 or Article 5.

5. Article 5A(i) – Is it the intention of the Law to hold someone accountable for the actions of a second party, and what safeguards are in place to protect legitimate businesses who may sell duel use items? (Is there a way of determining that the seller did not know the intentions of the second party?)

See point 4 above. Were there to be some question that a "dual use item" was used in the commission of an offence, that case would be decided on its own facts as to whether those involved intended that the item would be used to commit an offence under the Law. (See also Article 5A(2), which says that a person is guilty of an offence if *"he or she supplies or offers to supply any article in the commission of an offence under Article 2 or 5".*)

6. Article 5A(i) – Could security professionals be effective charged under the draft Law subject to intent?

Anyone can be charged under the Law if there is evidence that their intention has been to commit an offence.

7. Article 5A(i) – What consideration has been given as to whether this draft law will dissuade people from teaching and learning in this area?

Legislation equivalent to the Law is in place in any jurisdictions including the UK, so practitioners should have a good understanding of its implications. The central element of the relevant offences is intent, and so educational activities should be unaffected.

8. Computer Misuse (Jersey) law 1995 – As the draft Law does not define computer, what consideration has been given to the types of devices that this would include?

The Crown Prosecution Service in the UK has published guidance on the UK Computer Misuse Act, which is similar in purpose and approach to the 1995 Law. It advises that the Act "deliberately does not define what is meant by a 'computer', to allow for technological development". In DPP v McKeown and, DPP v Jones [1997] 2 Cr App R 155 HL, Lord Hoffman defined computer as 'a device for storing, processing and retrieving information'; this means that a mobile smartphone or personal tablet device could also be defined as a computer in the same way as a traditional 'desk-top' computer or 'PC'.

Similarly, in Jersey, allowing the Courts to define 'computer' in this manner is intended to allow the 1995 Law to survive unanticipated changes in technology.

9. Computer Misuse (Jersey) Law 1995 – Is the Law futureproofed to include smart devices (i.e. Amazon Alexa, Kettles, etc.)

Yes, for the reasons explained at 8 above, above, these devices would be within the scope of the Law.

10. Regulation of Investigatory Powers (Jersey) Law 2005, Article 42F – What process will be followed when requesting a key for a device from an individual?

The UK Home Office has published a Revised Code of Practice on the Investigation of Protected Electronic Information, dated August 2018. This sets out the process that must be followed in those circumstances by UK authorities exercising powers under the UK Regulation of Investigatory Powers Act ("RIPA"). Post-amendment, our domestic Regulation of Investigatory Powers Law ("RIPL") will be functionally very similar to the UK legislation, so there will be potential for the States of Jersey Police to consider the relevant Home Office guidance as it does in other areas of police procedure:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742064/RIPA_Part_III_Code_of_Practice.pdf

11. Regulation of Investigatory Powers (Jersey) Law 2005, Article 27A – Does this section of the Law cater for operators using contractors or third parties to carry out work?

The Law as it amends RIPL does not expressly refer to contractors or third parties carrying out work. The current version of RIPL simply refers to "postal or telecommunications operators" as meaning "*a person who provides a postal service or telecommunications service*" (Article 24)). Where there is any question as to whether a notice and its contents (as given to a postal or telecommunications operator) is to be

kept secret, Article 27A(8) is engaged. Here, a disclosure is defensible if it is made to the Commissioner or authorized – (a) by the Commissioner; (b) by the terms of the notice; (c) by or on behalf of the person who gave the notice; or (d) by or on behalf of a person who – (i) is in lawful possession of the protected information (within the meaning of Article 42A(1)) to which the notice relates, and (ii) came into possession of that information.".

12. Is it intended for there to be any guidance around the work of security practitioners, especially training in this field and around ethical security?

Not specifically in Jersey, but comparable provisions have been in place in the UK for over 10 years, so it is a reasonable assumption that most practitioners will have some understanding of the requirements.

13. What consideration has been given to the impact on someone's mental health if they are genuinely unable to remember an encryption password?

The offence of failure to comply with a notice (Article 42F) is only met when a person "knowingly" "fails to make the disclosure required by the giving of the notice and in accordance with the notice", such a test is fact-dependent in each case (Article 42F(3)). In corporate bodies, the notice might be addressed to multiple people, avoiding this issue.

14. Who is intended to be asked for access to systems within an organisation and what is the protocol for doing so?

In the context of a notice, Article 42B(5) requires that a senior officer of a body corporate shall be the recipient unless there is no such senior officer. Further, where more than one person is in possession of a key to any protected information (as employees of a firm), a notice may be given to any employee, unless there is a partner or more senior employee to whom it is reasonably practicable to give the notice.

15. Regulation of Investigatory Powers (Jersey) Law 2005, Article 27(A) – What is the intention of the Law in relation to third party contractors?

See answer to 11 above.

16. Regulation of Investigatory Powers (Jersey) Law 2005 – What is meant by economic well-being of the Island when seeking grounds to investigate a device and seek access to it?

The relevant authority will have to convince a Court that an action is 'in the interests of the economic well-being of Jersey', and the Court will decide if this is a valid claim on the particular facts and circumstances of the case. The 'economic wellbeing of the country' is identified in the ECHR as a reasonable ground for states to take certain actions, and the UK's Regulation of Investigatory Powers Act 2000 contains the same provision.

17. Does this legislation offer futureproofing against technology such as Artificial Intelligence and the Internet of Things?

In respect of the 'Internet of Things', as per question 8, the two safeguards are (a) the current definition of "computer", which is wide enough to capture any data storage device, and (b) the capacity of the Courts to interpret 'computer' as needed. If a 'Thing' has sufficient capacity to be WiFi enabled it is likely to be a 'computer' under the Law, and if it is not it must be controlled by something that is a 'computer'. Accordingly, unauthorized access to, for instance, an internet-enabled refrigerator will, prima facie, be a crime under the Law.

Regarding 'Artificial Intelligence', any AI with data storage capacity will be treated as a computer system. There may be significant questions around AI culpability and policing of AI generated activity, but these are wider questions for the justice system to consider.

18. Can the authorities demand a key to data that has been obtained unlawfully?

Yes.

19. What if decrypting a drive provides access to significant other information not related to the investigation? How will this be managed?

Sensitive information that does not relate to a criminal offence will be treated in complete confidence. Evidence that points to other offences will be dealt with in the normal manner and may result in a prosecution for the relevant office. This is the case with evidence uncovered in physical searches, and is already the practice in relation to digital evidence. For instance, were a computer seized as part of an investigation into online grooming, and indecent images of children were discovered, then those images could result in a separate prosecution.