FOCUS

HIGGS & JOHNSON COUNSEL & ATTORNEYS-AT-LAW | VOLUME 61, ISSUE 1/2017

Cybercrime under Bahamian law

By Portia J. Nicholson

Accusations of Russian hacking and WikiLeaks data dumps have once again directed our attention to the pervasive problem of cybercrime. Information technology is an indispensable part of our everyday lives, which, although invaluable, makes us all vulnerable to cyber criminals. From the professional networks used in business, to online shopping, online banking, mobile data services and social media networks, the use of cyber technology is nothing short of ubiquitous. Hand in hand with the growth of digital information has been the exponential increase in cybercrime and the bewildering array of security systems aimed at combatting it. So clearly, the problem is huge. And it will get even bigger.

To date, the only Bahamian legislation that addresses cybercrime directly is the Computer Misuse Act 2003 (the "CMA"). The CMA defines the term "computer" very broadly to include: (i) any electronic, magnetic, optical, electrochemical or other data processing device or series of interconnected devices performing logical, arithmetic, or storage functions; and (ii) any data storage facility or communications facility directly related to, or operating in conjunction with, such device or group of interconnected devices. So arguably a "computer" under the CMA would include devices such as smart phones, tablets, smart TVs, smart watches and perhaps even a microwave oven capable of conducting surveillance, if these exist. >>

The CMA criminalises actions which fall into the following categories:

- Using a computer to secure unauthorised access to any program or data held in a computer;
- Using a computer to secure access to any program or data held in any computer with intent to commit an offence involving property, fraud or dishonesty, or which causes bodily harm;
- Doing any act which you know will cause unauthorised modifications in the contents of any computer;
- Knowingly (i) securing access without authority to any computer for the purpose of obtaining any computer service, or (ii) intercepting without authority any computer functions using any device, or (iii) using or causing a computer to be used directly or indirectly for the purpose of committing an offence;
- Knowingly and without authority or lawful excuse interfering with, interrupting or obstructing the lawful use of a computer; or impeding or preventing access to, or impairing the usefulness or effectiveness of, a computer;
- Knowingly and without authority disclosing any password, access code or other means of access to any program or computer data for wrongful gain or an unlawful purpose or knowing that it would cause wrongful loss to any person; and
- Obtaining access to any protected computer in the course of commission of an offence.

With respect to item 7 of the offences listed above, a computer is a 'protected computer' if the offender knows, or ought reasonably to know, that the computer or program or data is used directly in connection with, or is necessary for the:

- security or defence of international relations of The Bahamas;
- existence or identity of confidential informants relating to criminal law enforcement;
- provision of services relating to communications infrastructure, banking, and financial services, public utilities, public transportation or key public infrastructures; or
- protection of public safety including essential emergency services such as police, army and medical service.

Under the CMA, any person who incites, solicits or abets the commission of any offence is also guilty of that offence and liable to the full punishment.

It is clear that the CMA criminalises the most common forms of cybercrime, including *hacking* of the sort complained of by the US Democratic National Committee, the common *phishing* scams aimed at entering your bank account, and *spoofing* emails purporting to be from reputable companies in order to induce you to reveal to the spoofer personal information, such as passwords and credit card numbers. The CMA also covers offences such as cyberstalking, cyberbullying, unlawful online gaming and online prostitution.

The offences under the CMA are not limited to activities which utilise one computer to gain access to another. A person who walks into your office, sits at a computer and begins to access or alter data without authority would be as guilty of an offence under the CMA as someone who emails you malware in order to alter or damage your program or data.

Further, English case law has established, in relation to legislation similar to the CMA, that causing a computer to record data may amount to a modification of the computer. Further, where access to a computer is granted, the use of such access for a purpose which is not authorised will constitute unauthorised access.

The CMA applies extraterritorially and empowers the Bahamian courts to exercise jurisdiction in relation to any offence committed outside of The Bahamas, whether by a Bahamian or a foreigner if either the accused, or the computer, program or data was in The Bahamas at the material time.

It is comforting to know that there is some protection from cyber criminals under Bahamian law. However, as new technologies and new forms of criminality emerge, it may become necessary to update the legislation. Further, the enforcement of the provisions of the CMA will undoubtedly give rise to various issues. For example, the use of law enforcement powers could adversely affect innocent victims and their data protection rights; the fragility and ease of modification / destruction of digital data may lead to difficulties with identification, collection, storage, preservation and adducing of digital evidence; extra-territorial enforcement will test the effectiveness of mechanisms for international cooperation between law enforcement agencies; and inter-jurisdictional differences may stymie law enforcement attempts.

Finally, based on judicial decisions elsewhere, public interest in the disclosure of hacked information may be held to outweigh private property and data protection rights, so that a person who commits an offence under the CMA may nevertheless have the satisfaction of succeeding in his end game if the courts refuse to restrain the disclosure of the illegally obtained data.

Portia J. Nicholson is Partner in the firm's Corporate and Commercial Practice Group with over 25 years of experience in the areas of Corporate and Commercial law. She has acted as counsel in many domestic commercial projects and has served as special counsel in respect of numerous cross-border financing transactions and corporate restructuring projects.

pnicholson@higgsjohnson.com