ARTHUR COX

Group Briefing
March 2016

Cybercrime Legislative Developments in Ireland

KEY CONTACT

For further information please speak to your usual Arthur Cox contact or:

PEARSE RYAN
PARTNER
+353 1 618 0518
pearse.ryan@arthurcox.com

TOM BROWNE
ASSOCIATE
+353 1 618 4367
tom.browne@arthurcox.com

SARAH MCDERMOTT
TRAINEE
+353 1 618 0000
sarah.k.mcdermott@arthurcox.com

INTRODUCTION

On 15 January 2016 the Government introduced the long awaited Criminal Justice (Offences Relating to Information Systems) Bill 2016. The purpose of the Bill is to give effect to the provisions of Directive 2013/40/EU of 12 August 2013 on attacks against information systems (the deadline for transposition of which was August 2015).

Currently, the law on cybercrime in Ireland is contained across a number of legislative acts, namely the Criminal Damage Act, 1991 (the "1991 Act"), the Criminal Justice (Theft and Fraud Offences) Act, 2001 (the "2001 Act"), and the Criminal Justice Act 2011 (the "2011 Act"). Apart from the 2011 Act, which was introduced for particular purposes in support of An Garda Síochána (the national police force) investigations, the substantive law in Ireland, set out in the 1991 Act and 2001 Act is elderly, contains notable omissions and is seldom used as the basis for prosecution. The substantive law has been discussed previously.[1]

The 2011 Act was introduced primarily to facilitate Garda access to information and documentation in the course of an investigation. While it is an effective piece of legislation (which is the subject of previous discussion[2]) it is largely procedural in nature. Consequently, it has been fifteen years since legislation was enacted which addressed cybercrime specifically, or any substantive offences in the area were introduced. In the context of the technological developments of the last 15 years, the Bill is necessary to update the law in the area and aims to offer greater protection to modern information and communication systems.

This article sets out a brief summary of the more noteworthy provisions of the Bill. Subsequent articles will discuss the substantive provisions of the ultimate Act, including any noteworthy changes to the text of the Bill. We discuss the status of the Bill below.

DEFINITIONS

The Bill removes cybercrime entirely from the remit of the 1991 Act, amending the 1991 Act to remove all references to data and cybercrime offences. The Bill also introduces a new definition of data, replicating the definition set out in the Directive. Data is defined as:

1. See Society for Computers & Law website - http://www.scl.org/site.aspx?i=ed16653
2. See Society for Computers & Law website - http://www.scl.org/site.aspx?i=ed29676

"any representation of facts, information or concepts in a form capable of being processed in an information system, and includes a programme capable of causing an information system to perform a function"

Currently, cybercrime offences in Ireland centre on actions involving a 'computer', which is undefined in the legislation, effectively allowing law enforcement, through the tools of statutory interpretation, to keep pace with technological developments. The Bill introduces the concept of an 'information system', defined, again reproducing the definition in the Directive, as:

"(a) a device or group of interconnected or related devices, one or more than one of which performs automatic processing of data pursuant to a programme, and

(b) data stored, processed, retrieved or transmitted by such device or group of devices for the purposes of the operation, use, protection or maintenance of the device or group of devices, as the case may be."[3]

NEW SUBSTANTIVE OFFENCES

Section 3 of the Bill creates the offence of interference, by way of hindering or interruption, with an information system without lawful authority. This offence addresses for the first time in Irish law denial-of-service attacks on information systems, which prevent legitimate users from accessing information or services which rely on the affected computer or network. The express omission of DOS type attacks is one notable omission from the scope of existing legislation.

The Bill further introduces in section 5 the offence of intentionally intercepting any transmission of data, without lawful authority, from or within an information system. [4]

Section 6 of the Bill makes it an offence to produce, sell, procure for use, import, distribute, or otherwise make available the tools that can be used to commit the offences set out in the Bill, for the purpose of the commission of an offence under the Bill. It is the intention of the Directive that such tools could include malicious software, including those able to create botnets, used to commit cyber-attacks.

This article does not discuss transnational jurisdictional issues, which is a feature in almost all substantive cybercrimes.

REPEALS AND AMENDMENTS

Under section 5 of the 1991 Act, which is repealed under the Bill, it is an offence to operate a computer with the intent of accessing data, even if the data is not in fact accessed. Section 2 of the Bill steps into the void created by the repeal of section 5, creating the offence of intentionally accessing an information system without lawful authority.[5]

Section 4 of the Bill addresses the interference with data on an information system without lawful authority, including the intentional deletion, damaging, alteration or deterioration of data on an information system. The Bill repeals the constituent parts of section 2 of the 1991 Act, which provided for the offence of damaging data, and section 4 of the Bill mirrors the effect of the repealed provisions.

SEARCH WARRANTS

The Bill provides under section 7 that a District Court judge may issue a search warrant for the search of any place that a member of an Garda Síochána has reasonable grounds for suspecting that evidence relating to the commission of an offence under the Bill may be found.

Notably, section 7 further provides that failure to comply with a requirement to give certain information to the member acting under the authority of the search warrant, including giving any password, encryption key or code necessary to access information held on a computer, shall be guilty of an offence. These measures to ensure compliance are in addition to the provisions of the 2011 Act. They are noteworthy law enforcement type provisions.

PENALTIES

A person convicted of an offence under sections 2,4,5 or 6 shall be liable on summary conviction to a EUR5,000 fine or imprisonment for a term not exceeding 12 months, or both, and on conviction on indictment to an unspecified fine, or imprisonment for a term not exceeding 5 years, or both.

An offence under section 3 carries a penalty of a EUR5,000 fine or imprisonment for a term not exceeding 12 months or both on summary conviction, and on conviction on indictment, to an unspecified fine or imprisonment for a term not exceeding 10 years or both.

A person convicted of an offence under section 7 shall be liable on summary conviction to a EUR5,000 fine, or imprisonment for a term not exceeding 12 months, or both.

The Bill further provides that in imposing a sentence in respect of section 3 or 4 the Court may regard as an aggravating factor the fact that the offence was committed by misusing the personal data of another person, with the aim of gaining trust of a third party, thereby causing prejudice to that other person. This reference to social engineering is a noteworthy extension of the law.

3. This definition is arguably more suitable to a computer based information system or computer information system than the potentially broader information system.
4. It is quite likely future prosecution arguments will turn on the meaning of 'lawful authority'.
5. In practice, proving intention can be difficult.

NEXT STEPS

As the Bill was only introduced on 15 January 2016, it has not yet reached the second stage in the introduction of legislation, and as such has not yet been debated in the Dáil. The Dáil has not indicated when this second stage might take place. There are five stages in total through which a bill makes the passage from bill to act, with no upper limit on how long this process can take. Given that as we write this a general election has recently taken place, which has produced an inconclusive result, it may be some time before a Government is formed and the legislative process continues. [6]

The Bill is a welcome updating of the law on computer crime and computer aided crime in Ireland. It remains to be seen when the Bill will be enacted and what changes it will undergo as it winds its way through the legislative process.

6. General Election 2016 – 4th March 2016