CS 978 – Legal, Ethical, and Professional Issues for the Information Society

Lecture 6 – Computer misuse legislation

Introduction

Legislation in the UK that deals with computer misuse goes back as far as 1990, and indeed it is still the Act passed then that largely governs criminal law in the area, for instance, theft for any crime involving stealing using the technology.

This week we will discuss the Act and the activities it deals with, as well as updates to the Act passed in recent years to deal with increasingly new crimes.

The need for a specific Act

Legislation related to computer misuse in the UK did not appear until relatively late, from the point of view of the development of computers and their impact on society. Before 1990, any crimes that were committed using computers were usually charged under the legislation related to the crime itself: this led to some peculiar cases. For instance, a case involving deleting of data from magnetic computer disks had to be interpreted under the Criminal Damage Act, and the notion of damage had to be interpreted in a new way, i.e. damage to the digital contents of a disk rather than the disc itself. Another potential act used was the Theft Act 1968 which made abstracting of electricity a criminal act. There was some thought that criminals using computers to carry out their crimes could be charged for the electricity they stole!

Things reached a head in the case of R v Gold and Schifreen, where the defendants were charged under the Forgery and Counterfeiting Act for illegally accessing an online information service called Prestel which was in use by companies in the early 80s. This was in the days before the Internet, and the use of such databases was very expensive.

In the R v Gold and Schifreen case, the defendants were found guilty, but it was quashed on appeal. The appeals judges believed that the law used to prosecute the men was not appropriate for the crime they had committed, as they stated:

> "We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case."

It was evident then that technology had raced ahead of the law and that legislation related to computer misuse was now vital. With the growth in computers and their power to undertake transactions across international boundaries, there was indeed a massive hole opening in terms of the ability to challenge computer crime.

The Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) defines three types of computer misuse offence. These are:

1. Unauthorised access to computer material
2. Unauthorised access with intent to commit or facilitate the commission of further offences.
3. Unauthorised modification of computer material

1.Unauthorised access to computer material

This first part of the act deals with the initial unauthorised access to a computer. Put simply it is an offence under the law to access any computer without permission if the offender knows that the access is unauthorised. This is why you see on many computer networks the addition of what is known as log-in banners, where a user has to agree to access the network by clicking a button to confirm they are authorised to access the network. In other words, if a user does not know they should not be using that computer/network then it is not necessarily illegal. The onus is on the computer or network owner to make it clear to anyone accessing it that they have agreed to the conditions of use.

In this part of the act, the accessing of the computer/network itself is all it takes to break the law. It does not matter what the user is intending to do, or what they actually do when logged on. To break this part of the act, the unauthorised access itself is illegal. Punishment for this offence was up to six months in prison or a fine of £5000.

2.Unauthorised access with intent to commit or facilitate commission of further offences

This second offence in the act relates to the intention to commit further offences once access to the computer/network has been obtained. For instance, accessing a network to undertake some theft or other fraudulent activity would be a crime under this section of the act. An example might be accessing someone's internet banking account or similar to steal money. Doing so would breach part 1 of the act, and also part 2.

Punishment for this offence was up to 5 years imprisonment or a fine.

3.Unauthorised modification of computer material

The third offence relates to the modification of content on the computer once accessed. The offences encompass activities that might impair the operation of the computer, or prevent or hinder access to the computer, or impair the operation of a program(s) or the reliability of data. Some example crimes in this section could include accessing a computer/network and restricting access to others, such as is seen in some of the Microsoft scams where people receive cold calls telling them their computer is malfunctioning and to pass on access to a fraudulent administrator, who then locks access to the computer until a sum is paid. Another example might be logging on to a system to change data within it .

Challenges with the Act

The Act remains in law to this day, however, it has been amended in recent years as we will see. One of the issues with any act relating to computer crime is that the crimes can evolve, and the law can sometimes fail to catch up. Some real cases illustrate the challenges posed by the Act in the modern era, especially around dedicated denial of service attacks (DDoS).

In R v David Lennon, the defendant pleaded guilty under Section 3 of the Act, after sending 5,000,000 emails to a former employer in a DDoS attack. His pleading guilty was after the case had originally been thrown out after a judge had decided that sending the emails to crash the server could not be deemed to constitute “unauthorised modification of a system”.

In R v Aaron Caffrey the defendant was acquitted after being charged under Section 3 of launching a DDoS attack on the computer system of Houston’s port authority. He argued in the case that is computer had bene taken over by a Trojan virus without his knowledge.

With DDos attacks becoming more common, the government was keen to make this aspect of law clear. In addition, it was also felt that some of the punishments for the offences conceived in 1990 were no longer severe enough to deter offenders.

Updates to the Act

Two pieces of legislation updated the CMA, the Police and justice Act 2006, and the Serious Crime Act 2007. The changes they made were:

- The penalties for Section 1 were increased from 6 months to 2 years, making it eligible for extradition from foreign countries.
- The statutory limitations were abolished, meaning there was now no limit on when someone could be charged with arrest (the previous limit was 6 months). Secondly there was now no limit on when someone could be charged after the offence occurred (the previous limit was 3 years).
- DDoS attacks were made illegal, with up to 10 years imprisonment as potential punishment
- It was made illegal to distribute tools that could be “likely” be used to hack into a network. This point was controversial as it concerned researchers and others engaged in legitimate hacking, though it has not been interpreted as applying to ethical hacking.

Conclusions

In the UK recent legislation aimed at amending a decades-old Act is putting in place much stricter punishments. It has attempted to catch up with the potential damage computer crime can now inflict on individuals, corporations, and even countries. Nevertheless, the updates have drastically raised the stakes in terms of punishment for computer crimes, and we may well see other offences added to the mix as computers continue their rise in the prominence of societies.

Further reading

Adams, Andrew A. and McCrindle, Rachel J. (2008) *Pandora's Box: social and professional issues of the information age*. Chs. 11 and 13

DMcM/09-2017