# Current sentencing trends for data protection and data 'theft' offences

16/10/2015

**Corporate crime analysis: What are the current trends in the court when it comes to issuing its penalties in this area? Jacqueline Zoest, an experienced barrister and specialist in cybercrime law at Carmelite Chambers comments on the latest trends.**

## Original news

Former Morrisons auditor guilty of data theft, LNB News 20/07/2015 156

*Andrew Skelton, a former employee of Morrisons supermarket has been sentenced to eight years for stealing personal data belonging to nearly 100,000 Morrisons employees. Mr Skelton was found guilty of fraud, securing unauthorised access to computer material and disclosing personal data.*

## What have been the main or newsworthy cases around data 'theft' in recent years?

In 2014, a 39-year-old man was convicted of 'stealing' bank and credit card details, having been charged under the Fraud Act 2006, s 6 (FrA 2006) and the Computer Misuse Act 1990, s 2 (CMA 1990). On appeal, a total sentence of two years' imprisonment was substituted for the original three-year sentence.

In 2011, a man was charged under CMA 1990 after hacking into the Facebook account of a minor celebrity--accessing her emails and offering to sell to the media the information obtained. On appeal, his 12-month prison sentence was reduced to eight months (See *R v Mangham* [2012] EWCA Crim 973)

In March 2012, four private investigators received jail sentences for obtaining data by deception under FrA 2006. They accepted commissions to obtain information by deception from banks or building societies.

Two T-Mobile employees, David Turley and Darren Hames, who sold customer data were given a conditional discharge in June 2011. However, they were ordered to pay £73,700 under the confiscation provisions of the Proceeds of Crime Act 2002.

## What do the cases tell practitioners about how the courts deal with data 'theft'?

There are a number of possible charges that can be brought where unauthorized data access or data 'theft' by individuals is concerned. Most commonly, these cases are charged as computer misuse under CMA 1990 and/or fraud under FrA 2006. Less frequently, an offence under the Data Protection Act 1998 (DPA 1998) is charged. Other options, depending of course on the facts of the case, are a charge of misconduct in public office or charges under the Regulation of Investigatory Powers Act 2000 (RIPA 2000).

Computer misuse under CMA 1990

Each of the offences under CMA 1990 has different components and correspondingly different higher maximum penalties. The offences under CMA 1990, s 1 and 2 are most often charged in data 'theft' cases:

- s 1 offence --unlawful access or hacking has a maximum penalty in the Crown Court of a two-year prison sentence or an unlimited fine, or both
- s 2 offence--unauthorised access with intent to commit further offences has a maximum sentence of five years in prison--again with an unlimited fine in the Crown Court
- s 3 offence--unauthorised acts with intent to impair the operation of a computer--used for example in dealing with a denial of service attacks--carries a maximum sentence of ten years in prison or an unlimited fine, but is perhaps less relevant in this context

On the other hand, a new offence under CMA 1990, which is potentially relevant in the context of data 'theft'-- a new s 3ZA offence--unauthorised acts causing, or creating risk of, serious damage (inserted by the Serious Crime Act 2015)--carries a sentence of 14 years' imprisonment, or life imprisonment where damage or risk thereof is to national security or

human welfare. One could envisage a situation where this new offence could be charged in a data 'theft' case, for example in a case of unauthorised access to sensitive data which is then released or published to the detriment of national security.

It should be noted that there are no specific sentencing guidelines relating to offences under the CMA. What we do have, however, is guidance from cases that have reached the criminal division of the Court of Appeal in relation to prosecutions under CMA 1990. In these, the sentence has varied not only with the CMA 1990 provision charged, but also with the number of charges and the cost to remedy any data breach. Some examples include:

- *R v Baker (Oliver)* [2011] EWCA Crim 928--the offender was a disgruntled former employee sentenced to four months' imprisonment under CMA 1990, s 1
- *Mangham* [2012]--the six-month prison sentence for offences under both ss 1 and 3 was reduced on appeal to four months--strong mitigation put forward in relation to the defendant's Asperger's Syndrome, but with the aggravating factor of the cost to Facebook of $200,000 to fix its system
- *R v Crosskey (Gareth)* [2012] EWCA Crim 1645--offences were charged under both s 1 and 3 where a minor celebrity's Facebook account had been hacked, her emails accessed and offers made to the media to 'sell' the information obtained--on appeal, a 12-month prison sentence was reduced to eight months, but the court rejected outright the idea of a suspended prison sentence

Offences under FrA 2006

These are charged where fraud is made out on the facts of the case. Like offences under CMA 1990, s 3, the maximum penalty is ten years in prison or an unlimited fine or both. Unlike the CMA 1990 however, detailed sentencing guidelines have been issued by the Sentencing Council--these are the 'Fraud, Bribery and Money Laundering Offences Definitive Guideline' and apply to England and Wales only.

The main FrA 2006, s 1 offence can be committed in three ways:

- false representation--s 2
- failing to disclose information--s 3
- fraud by abuse of position--s 4

In *Skelton*, the defendant was convicted of the s 4 offence and was sentenced to eight years' imprisonment.

*Unlawful data obtaining /disclosing under DPA 1998, s 55*

Prosecutions for unlawful obtaining can only be initiated by the Information Commissioner's Office (ICO) or with the consent of the Director of Public Prosecutions. The s 55 offence was designed to address the growth in private investigation agencies offering services based on the acquisition of such information. There is a £5,000 maximum fine on conviction in a magistrate's court and the potential for an unlimited fine if a case is brought in the Crown Court. It is implicit in this offence that either the defendant himself, or someone else, may have misused a computer--which is a more serious offence--prior to the data being obtained or disclosed.

Although the Criminal Justice & Immigration Act 2008, s 77 (CJIA 2008) empowers the Secretary of State for Justice to increase the maximum penalty by statutory instrument to a sentence of up to two years prison in the Crown Court--to date no such order has been made. The first prosecution in November 2002 in the Crown Court at Kingston in Codrington related to a benefits agency employee who had offered to sell personal data that had been unlawfully obtained.

In *R v Rooney* [2006] EWCA Crim 1841, AII ER (D) 158 (Jul) Bean J upheld on appeal a fine of £700 for a s 55 offence where the appellant had obtained Police National Computer (PNC) data in relation to the appellant's sister and a police officer she was having a relationship with after a planned wedding had been called off.

The ICO publishes details of s 55 convictions and penalties. These include:

- a £500 fine and £264.08 in prosecution costs for a former branch manager for Enterprise Rent-A-Car who 'stole' the records of almost 2000 customers before selling them to a claims management company in July 2014
- a £200 fine to an estate agent who attempted to access via telephone the account of a benefit claimant

- a £200 fine to a former member of the British National Party who posted the party membership list on the internet in November 2008
- a £800 fine and £400 costs for a bank cashier who accessed the bank account details of a woman who had accused her husband of sexual assault
- a £1,050 fine and £1,160 costs for a NHS worker who passed on patient details to her boyfriend who worked for a personal injury claims management company

*Misfeasance in public office*

A number of the reported cases on misfeasance in public office have to date involved police officers using data on the PNC for their own purposes. What all the cases have in common is that these sorts of data breaches invariably result in an immediate prison sentence for the offender whatever mitigation is presented. Reported cases show sentences of imprisonment from nine months to four years. Where PNC data has been sold or used for commercial gain or where the safety of members of the public has been put in jeopardy, then the sentence has been towards the upper end of the scale. In *R v O'Leary* [2007] EWCA Crim 186, Longmore LJ in the Court of Appeal said the starting point for a sentence, subject to mitigation, was an immediate prison sentence of four years.

## So what can we conclude about current trends in this area and does this assist us in defending data protection/data 'theft' prosecutions?

It is difficult to identify any real trend across the various cases and examples mentioned above. As can be seen, much depends on how the offence is charged and who is prosecuting.

ICO prosecutions are at the lowest level--the likely outcome is a fine in the magistrates court. On the other hand, a public sector worker--or former one--such as a police officer facing charges for misfeasance in public office is likely to receive an immediate prison sentence from the Crown Court if convicted.

The outcomes of CMA 1990 offences are more varied--perhaps due in part to the absence of formal sentencing guidelines. The most likely outcome of a s 1 offence is a custodial sentence measured in months, whereas a s 2 or s 3 offence will carry a longer custodial sentence. There are CMA 1990 cases where the sentence of imprisonment has been suspended--this offers hope to those defendants with compelling mitigation--in addition to a guilty plea.

As we have seen, FrA 2006 offences have clear guidelines as to sentence with tables based on financial loss together with aggravating and mitigating factors to be considered.

It is fair to say that it is difficult to draw any conclusions around sentencing trends for data 'theft' offences, partly because the reported cases vary widely on the facts and on the offences charged. What is clear is that prosecutors have become more adept at charging these offences in such a way as to maximize the sentencing powers available to the courts.

Anyone charged with a data 'theft offence would be well advised therefore to engage a barrister or solicitor experienced in criminal law, cybercrime and fraud and who has sufficient understanding of the technical issues involved properly to review the evidence. As always, the prosecution has to prove its case. This requires the prosecutor to produce considerable technical evidence as to who accessed what, when and how this was done. Defendants therefore require a defence team who are able to review vast quantities of often technically complex evidence in order properly to advise on the strength of the case and on likely sentence if convicted.

*Interviewed by David Bowden.*

*The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor*