Data Protection Act 1998

Monetary Penalty Notice

Dated: 9 May 2011

Name: Andrew Jonathan Crossley trading as ACS Law

Address: 20 Hanover Square, London W1S 1JY

Statutory framework

1. Andrew Jonathan Crossley trading as ACS Law is the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by Andrew Jonathan Crossley trading as ACS Law and is referred to in this notice as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1)(a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties) (Maximum

Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

1. Since early 2009 the data controller, a sole practitioner of the legal practice ACS Law, has specialised in pursuing alleged copyright infringement cases on behalf of corporate copyright holders. Several of the data controller's clients deal in films containing adult content; others control copyright in music tracks and computer games. IP ("Internet Protocol") addresses associated with alleged infringing activities were sent by email to the data controller by copyright owners or their tracking companies. The names and addresses of the internet

account holders allocated to those IP addresses at the precise time and date stated were then requested from the Internet Service Provider ("ISP"). ISPs would not normally provide the relevant data without an Order from the Court obtained by the data controller. Once an Order had been served the ISP would then send the requested information to the data controller, in most cases by unencrypted or non-protected email with an attached spreadsheet.

2. The Commissioner understands that the data requests sent to each ISP by the data controller were for information populating a spreadsheet containing hundreds, and sometimes thousands, of IP addresses. These spreadsheets stated not only the precise time and date of the alleged infringement, IP address and ISP, but also the name of the copyright holder and the work subject to the copyright. As stated above, many of these works were films containing adult content. ISPs responded to the data controller by returning the spreadsheet with all of the existing data, together with the name and address of the registered account holder that they had input alongside each entry.

3. After sifting and recording this data on his case management system, a bulk printing firm was contracted by the data controller to print and send standard letters to several thousand named individuals at a time, alleging that their internet connections had been used to infringe copyright and suggesting a compromise settlement. The Commissioner received 34 complaints and 27 enquiries about the data controller before the incident described in this Notice and which occurred in September 2010. As early as Spring 2009 comments appeared on web forums about the possibility of a distributed denial of service ("DDOS") attack against the data controller's IT and office systems. The data controller's actions were also criticised in the House of Lords during debates on the Digital Economy Bill.

4. The Commissioner understands that a number of the individuals contacted by the data controller entered into a compromise agreement even though they did not accept that their internet connections had been used to infringe copyright. The data controller sometimes negotiated with individuals entering into compromise agreements by allowing payment by instalments or reducing the amount the individuals were required to pay. The data controller also had guidelines for discontinuing cases in relation to elderly or infirm individuals and those with notified chronic or serious illnesses or impaired mental health subject to certain criteria being met. To this end a number of the individuals wrote to the data controller offering such evidence. These letters would then be scanned and attached to emails between the data controller's staff, as part of the process of producing and authorising further correspondence with the individual.

Also attached to such emails were payment forms, showing individuals' credit card details, and other correspondence from those contacted, some of which included references to sexual life, health or financial status.

5. Early in 2009, the data controller decided that his former web-hosting company was no longer able to meet his ongoing business needs as he was experiencing significant downtime with his web-pages and email accounts. The data controller instructed one of his legal assistants to research and recommend a new web-hosting company and package to him. Neither the data controller nor this legal assistant had any IT qualifications. The legal assistant did a basic search on the internet to find potential web-hosting companies and came across a web-hosting company (the "web-host") which he recommended to the data controller on the basis that it offered online customer service and a program that allows individuals with limited computer programming knowledge to create web-page templates or to amend web-pages easily.

6. In April 2009, the data controller decided to use the web-host as his new internet and email host and entered into a contract with it for what it described as a "home" web-hosting package at a cost of £5.99 per month. It is clear that this package was not intended for significant business use. Further, the "shared server" package provided by the web-host did not appear to provide any guarantees to the data controller in relation to the security of the personal data referred to in paragraphs 2 and 4 above.

7. In late September 2010, the data controller's web server was targeted for a DDOS attack by an online group of activists. Although this form of attack is illegal in the UK, the "distributed" element of it means that individuals from around the world can take part. The "denial of service" element means that hundreds or thousands of individual requests for access are constantly made to the targeted website, resulting in the server hosting it going offline under the strain. The aim of a DDOS attack is not to gain access to the server, but to deny access to the targeted website for any legitimate traffic, potentially resulting in the loss of business.

8. In this case, the data controller's website was taken offline and suspended by the web-host to prevent the DDOS attack from compromising the web-host's other client accounts hosted on the same server but at some point after the DDOS attack had begun, a file containing all the emails from the data controller's accounts was made available on a torrent site and from there, shared and distributed to other sites. Any person accessing the torrent site was then able to

read and download the spreadsheets and other attachments to emails referred to in paragraphs 2 and 4 above. The Commissioner estimates that at least 6,000 individuals were affected when the data was leaked online.

9. Following the incident and press reports the data controller reported this matter to the Commissioner's office and other relevant bodies. He also discontinued his contract with the web-host, and ISPs stopped responding to his requests for information until they could be reassured as to the security of the data once transferred. Email capability from the data controller's computers was disabled and electronic transfers of data were stopped. The data controller also commissioned a former client, with IT/business analysis skills, to conduct a formal review of his IT systems and processes and recommend any changes or improvements. This resulted in a report entitled "Business Systems Review" dated 11 October 2010 which made over 20 recommendations, including basic elements such as the installation of a firewall and access control.

10. In particular, the report recommended that the data controller should employ a professional individual or a third party company to manage his IT security and that this person should regularly re-evaluate his security. The report was also critical of the data controller's level of IT security and the technical skills of the staff used to manage the IT systems. The data controller states that he has spent approximately £20,000 as a result of this incident. Further, the data controller has now ceased the business activity that led to the attack on the web server, resulting in a loss of revenue and the jobs of 14 of 16 employees. He states that he has also taken additional steps to improve security. As a result of this incident the Commissioner received a further 35 complaints and 4 enquiries about the data controller, although a press release may have helped to stem any further complaints.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Paragraph 9 at Part II of Schedule 1 to the Act provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected".

Paragraph 11 at Part II of Schedule 1 to the Act provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

Paragraph 12 at Part II of Schedule 1 to the Act further provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-

(a) the processing is carried out under a contract-

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle in relation to all personal data with respect to which he is the data controller.

In particular, the data controller failed to take appropriate technical and organisational measures against the accidental loss of personal data. The data controller used a legal assistant who had no IT qualifications to research and recommend a new web-hosting company and package to him. The legal assistant did a basic search on the internet to find potential web-hosting companies and came across the web-host, which he recommended to the data controller on the basis that it offered online customer service and a program that allows individuals with limited computer programming knowledge to create web-page templates or to amend web-pages easily. There appears to have been no consideration of the security of the personal data referred to in paragraphs 2 and 4 above.

In addition, the data controller entered into a contract with the web-host for a "home" web-hosting package with shared servers at £5.99 per month. This was not intended for significant business use. The Commissioner considers that the data controller should have taken professional IT advice about an appropriate web-hosting company and the implementation and development of his associated IT systems. At the very least the data controller should have subscribed to a web-hosting package that was suitable not just for businesses generally but for the specific nature of his business.

Further, the data controller failed to comply with the Seventh Data Protection Principle, paragraphs 11 and 12 at Part II of Schedule 1 to the Act.

The contravention is serious because the measures taken by the data controller did not ensure a level of security appropriate to the harm that might result from such accidental loss and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress. The data controller's failure to comply with the Seventh Data Protection Principle was likely to cause substantial damage and/or substantial distress to data subjects whose personal data and sensitive personal data have been disclosed to third parties.

  In this particular case, the names and addresses of some of the individuals were linked with the illegal file sharing of films containing adult content, and some of those deny either uploading or downloading the files. Other personal data and sensitive personal data about individuals' financial and personal circumstances, including their

financial standing, credit card details, medical conditions and sexual life, have also been disclosed to third parties. The data subjects are likely to have suffered substantial distress, knowing that their personal data and sensitive personal data have been disclosed to third parties. If the data has been disclosed to untrustworthy third parties or relatives and acquaintances, then it is likely that the contravention would cause further distress and also substantial damage to the data subjects, such as exposing them to identity fraud or causing damage to their personal reputations and relationships. The situation is exacerbated by the fact that the personal data has now been disseminated worldwide on the internet and could be available to third parties indefinitely.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

  In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur. The data controller, whose business was routinely involved in handling large amounts of personal data in an internet-based environment, used a legal assistant with no IT qualifications to research and recommend a new web-hosting company and package to him. The data controller knew or ought to have known that failing to take professional IT advice about an appropriate web-hosting company and the implementation and development of his associated IT systems might lead to deficiencies in the data controller's IT systems, including the website and email accounts.

  Further, as early as Spring 2009 comments had appeared on web forums about the possibility of a DDOS attack against the data controller's IT and office systems, so he should have been on notice of the possible risk to his web server and stepped up security. There has also been extensive media coverage of instances of similar attacks on web servers. The data controller was well aware that his business was controversial and unpopular with some. He should have anticipated that it would come under attack and taken appropriate measures accordingly.

  The data controller was fully aware of the nature and amount of the personal data transmitted to and from ISPs by way of email attachment, so he ought to have known that such a contravention would be of a kind likely to cause substantial damage or substantial

distress to the data subjects.

The data controller failed to take reasonable steps to prevent the contravention because he failed to take professional IT advice about an appropriate web-hosting company and the implementation and development of his associated IT systems and, at the very least, he should have subscribed to a package with the web-host that was suitable not just for businesses generally but for the specific nature of his business.

In addition, the data controller failed to comply with the Seventh Data Protection Principle at paragraphs 11 and 12 at Part II of Schedule 1 to the Act.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

Nature of the contravention

- Contravention was serious because of the nature of the personal data and sensitive personal data
- Implementation of appropriate IT security measures could have prevented loss of the data

Effect of the contravention

- Large amount of personal data and sensitive personal data leaked online relating to around 6,000 individuals
- Personal data and sensitive personal data has been distributed worldwide and could be available to third parties indefinitely
- The contravention was of a kind likely to cause substantial damage and substantial distress to the data subjects

Behavioural issues

- Data controller had not taken any professional IT advice about setting up or developing and maintaining IT systems
- Data controller does not appear to have followed guidance published by the Commissioner in relation to data security, or complied with BS ISO/IEC 27001 on information security management
- Lack of proper IT controls had existed since February 2006
- Initially data controller was not fully co-operative with the Commissioner's office

- Data controller appeared to continue with his activities when he should have been aware of likelihood of attack
- Data controller is a lawyer and should have been fully aware of his obligations under the Act
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the accidental loss of personal data

Impact on the data controller

- Data controller made considerable savings in business overheads by not investing in IT advice and data security

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- Data controller obtained an injunction against two UK-based individuals involved in the attack and one limited company to prevent further dissemination of the data on the internet by them or on UK-based sites

Behavioural issues

- Voluntarily reported to Commissioner's office
- Some remedial action has now been taken
- Data controller has spent approximately £20,000 as a result of this incident
- Data controller is a small business and cannot be expected to have extensive in-house security expertise
- Data controller is now fully co-operative with the Commissioner's office

Impact on the data controller

- The data controller has now ceased the business activity that led to the attack on the web server, resulting in a loss of revenue and the jobs of 14 of 16 employees
- Liability to pay the monetary penalty will fall on an individual
- Significant impact on reputation of data controller as a result of this security breach

Other considerations

- The data controller failed to comply with the Seventh Data Protection Principle, paragraphs 11 and 12 at Part II of Schedule 1 to the Act

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data held on their web servers

Amount of the monetary penalty

The Commissioner considers that the contravention of section 4(4) of the Act is very serious and that the imposition of a monetary penalty is appropriate. Further he considers that were it not for the fact that the data controller is an individual with limited means a monetary penalty in the sum of £200,000 (Two hundred thousand pounds) would be reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

However, the Commissioner has considered the circumstances of the data controller together with written representations (sworn on oath) on the likely impact of this monetary penalty on him as an individual. In the circumstances the Commissioner has decided to impose a monetary penalty of £1,000 (One thousand pounds).

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 7 June 2011 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the

Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by 6 June 2011 the Commissioner will reduce the monetary penalty by 20% to £800 (eight hundred pounds).

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

b. the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on 6 June 2011 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

  In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court or any sheriffdom in Scotland.

Dated the 9th day of May 2011

Signed: 

Christopher Graham
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be served on the Tribunal by 5pm on 6 June 2011 at the latest.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).