CASE TRANSLATION: NORWAY

CASE CITATION:
HR-2012-2056-A

DATE OF DECISION:
31 October 2012

NAME AND LEVEL OF COURT:
Norges Høyesterett (Supreme Court)

MEMBERS OF THE COURT:
Judges Noer, Øie, Bårdsen, Bergsjø and Schei

Criminal offence; hacking; 'cloud' (online) storage of personal digital data; data protection; data controller; privacy

The Supreme Court – Judgement.

Criminal law. Data Intrusion. Application of the law. For purpose of gain. Privacy.

The penalty for violation of the criminal code § 145, second paragraph was set to imprisonment for one year, nine months were suspended. The defendant was convicted for breaking into private individuals' e-mail accounts, including downloaded intimate pictures, to have gained access to private information on a computer that he had been handed in for repair, and hacking to an American company by that he had downloaded large amounts of customer information. The requirement for purposes of gain, see Penal Code. § 145, third paragraph, was met by the defendant to the burglary who had acquired data on a variety of people, which were of economic value. When he had received a password and computer and had access to inspect machine in its entirety, he could not be convicted on the criminal code § 145 for having gained access to the data that were open to him. He was acquitted of the charges under the Personal Data Act, because he could not be considered a data controller by law. The requirement for publication under criminal code § 390 was not satisfied by the defendant's acquisition of data. Redress Claims for Damages Act § 3-6, then could not be awarded.

Delivered: 31.10.2012 in Case HR-2012-2056-A

Procedure: Oslo District Court TOSLO-2010-62157 – Court of Appeal LB-2011 – m102720 – Supreme Court HR-2012-2056-A, (Case No. 2012/969), criminal appeal against judgment.

Parties: I: The Public Prosecution (Attorney Geri Evanger – to try) to A (attorney Knut Helge Hurum – to try). II: A (attorney Knut Helge Hurum – to try) to the Public Prosecution (Prosecutor Geir Evanger – to try).[1]

Judges: Noer, Øie, Bårdsen, Bergsjø, Schei.

(1) Judge Noer: This case concerns a conviction for hacking. It raises questions about the interpretation of Penal Code § 145, second paragraph about the data breach, and whether the defendant acted for gain. Furthermore, the case deals with the question whether the defendant can be convicted for violation of the Personal Data Act, and whether the victim can claim damages for non-economic loss due to the violation of the right of privacy by data breach. There are also questions about compensation for financial losses.

(2) The Public Prosecutors Office initiated an indictment on 26 March 2010 against A for various allegations in connection that A had gained access to electronically stored information mainly through hacking.

(3) Indictment count I concerned violation of Penal Code § 145, second paragraph and had five subsections, where the principal points can be summarised as follows:

(4) Count I a concerned the penetration of one or more unknown servers, where the defendant had copied the information about the e-mail address, password and/or username and personal photos etc. Count I b concerned improper intrusion in 187 e-mail accounts and the retrieval of information and pictures from these. Count I c concerned the defendant obtaining access to private information on a computer that he had been handed over for repair. Count I d applied to hacking the server to the web site of the company Photobucket Inc, where the defendant had stolen the personal data, including user id, password, and e-mail addresses of over 66 million users. Count I e concerned hacking and retrieval of information

1 *'To try' (til prøve) in Norwegian refers to the fact that the lawyer in question (in this instance, each lawyer) is not authorized for Supreme court trials, and that this is a case in which the lawyer will try to be approved for and be evaluated for such approval.*

from the customer register of the company registered as Siteman AS.

(5) The defendant's motive for the actions was, according to the District Court's judgment, 'to obtain intimate pictures he would not otherwise have access to.' The defendant's four computers contained more than 30,000 images, including some that were pornographic in nature.

(6) A was also charged with violation of the Copyright Act and the Personal Data Act (counts II, III and IV). These items were primarily based on the fact that the defendant had copied and saved the same information.

(7) Oslo District Court ruled on 5 April 2011 (TOSLO-2010-62157). The defendant was sentenced in accordance with the charge (with the exception of part of count I e) to imprisonment for one year, whereof nine months were suspended. He was ordered to pay compensation to the company Photobucket Inc in the amount of 126,308.50 kroner and damages for non-economic loss to five victims of 30,000 kroner each. In addition, he was awarded court costs against to the public at 400,000 kroner.

(8) A appealed to the Borgarting Court of Appeal. The appeal concerned the application of law under conviction for the indictment of count I c, III and IV and the issue, of the sentencing for damages for non-economic loss, and the amount of compensation and the decision of the litigation costs.

(9) The Court of Appeal gave judgment on 30 March 2012 (LB-2011-102720) and acquitted the accused for item count I c, discounted the claims by Photobucket Inc to 109,325 kroner and acquitted the defendant of the claim for damages for non-economic loss. The costs of the court were reduced to 10,000 kroner. Otherwise, the appeal was rejected.

(10) The judgment is as follows:

> '1 A born *. * .1981, acquitted of the matters mentioned in the indictment count I c).
>
> 2. A is convicted for violation of Penal Code § 145 second ref first and third paragraphs (four issues), Copyright Act § 54, first paragraph, letter b), see third paragraph, the Personal Data Act § 48 subsection f), see § 20 cf. § 19 and Personal Data Act § 48 first paragraph letter a), ref § 31 first paragraph letter a) and second paragraph, all seen together with Penal Code § 62 first paragraph and § 63, second paragraph, to imprisonment for one – one – year. The enforcement of 9 – nine – months of the sentence suspended by Penal Code § § 52-54 with a probation period of two years.
>
> To offset in the unconditional part of the sentence is two – two – days spent in custody.
>
> 3. In compensation to Photobucket.com Inc, A shall pay compensation of 109,325 – one hundred and nine thousand three hundred and twenty five – Kroner plus statutory interest from the due date until payment is made. The due date is two weeks from the judgment.
>
> 4. A is acquitted for demands for non-economic damage from B, G, H, I and J.
>
> 5. A must accept the confiscation of a Linux server and a Silver Stone computer that were seized.
>
> 6. The costs to the district court are set to 10,000 – ten thousand – kroner."

(11) The Public Prosecutors Office has appealed to the Supreme Court over the application of the law on the question of guilt regarding the indictment on count I c and application of the law relating to the claims for compensation and non-economic damages. The defendant has appealed against the application of the law under conviction for count I a, b, d and e, count III and count IV. He also appealed against the application of the law in relation to the decision of the claim for monetary damages by Photobucket Inc. The appeals were fully taken under consideration by the Supreme Court.

(12) I have concluded that the appeals should partially succeed.

(13) *Count Ic – If A is punishable under the Criminal Code § 145, second paragraph for unjustified to have gained access to data*

(14) The reason for this indictment is that the aggrieved gave his computer and login password to the defendant so that he would fix virus problems on her computer. The defendant took the opportunity to go in and copy private information on the PC. The High Court referred to the court's description of the alleged offense, where the events are quoted as follows:

> 'Cohabitants to B is a work colleague with A. B had a laptop Fujitsu computer with which there was trouble. The cohabitant knew that A was clever with computers,

and has also helped others with such problems. The defendant agreed to help, and got the computer delivered at his home. They got it back not long afterwards.

Upon review of the seizure of the data made at A's, the police found the password of B to log into the e-mail account at getmail.no. The police also found the following information that was saved: her old e-mail address, her co-habitant's e-mail address, national identity number, the user name of her co-habitant's daughter and her e-mail address, account number and credit card number. The police also found photographs of B and her daughter, and the addition of her co-habitant's daughter. These were images that were stored on B's computer, but they were now also found as copies on the defendant's computer.'

(15) The question is whether the issues at hand are punishable under the Criminal Code § 145 first and second paragraph, which reads as follows:

'Anyone who illegally is breaking letter or other closed writing or in a similar way obtain access to the content, or makes his way to another person's locked repository, is punishable by fines or imprisonment for up to 6 months or both.

The same applies to a person who unwarranted makes his way to data or computer programs stored or transmitted by electronic or other technical means.'

(16) The prosecutor has alleged that the weight of legal interpretation must be in the 'unjustified' category: If the defendant was not entitled to obtain access to the stored data, and he still does, he has in the legal sense gained unauthorised access to the data and is affected by the provision. The defendant contends on his side that he was granted access to the PC and password. The information was then available to him, and he is in a legal sense given legitimate access.

(17) I consider that there is no doubt that the defendant by his actions was given access to 'data' within the meaning of the provision. The concept, according to the legislative history interpreted broadly 'includes all kinds of information, e.g. about the personal, technical or financial issues,' cf Ot.prp.nr.35 (1986-1987) on page 20. It is also clear that the provision applies to the gaining of access to the data – there is no requirement that the perpetrator is familiar with or has used the above information in any way.

(18) The second paragraph, however, affects only the person who 'without justification gains access' to stored information. To determine whether this condition is fulfilled here, I find it necessary to go any further into background of the provision.

(19) Penal Code § 145 originally referred to the illegally of breaking into a letter or a closed writing. But by Act of 16 February 1979 No. 3, a provision was added that made it a criminal offence to gain access to the contents of a closed communication or note when this was otherwise only available using special equipment to connect, play, screening, reading or the like. A condition for it being a legal offence was that the notice or record was 'closed', and that access was unauthorised, see Ot.prp.nr.4 (1978-1979) page 10.

(20) By Act of 12 June 1987 No. 54, § 145 was amended to the direction of the current wording, but with a requirement that unjustified access was obtained 'by violating a protection or in a similar way.' The amendment was intended to make clearer that the provision is directed against unauthorised access to computerised data, and was not meant to imply substantial changes of substance, cf Ot.prp.nr.35 (1986-1987) page 15.

(21) The provision was revised again by Act of 8 April 2005 nr 16. The Ministry proposed initially to maintain the requirement that the unlawful access must have occurred by breaking a protection or in a similar manner. However, Parliament removed the condition, and referred to a written submission from ØKOKRIM to the proposition for the revision, regarding the need to provide for information theft regardless of whether the offender violated a protective measure to obtain such access, cf Innst.O.nr.53 (2004-05) page 5. The condition that the person in question 'without justification gains access to data or programs' was nevertheless retained.

(22) The new data breach provisions in § 204 of the Penal Code of 2005 will replace § 145, second paragraph in respect of electronically stored information and reads:

'With a fine or imprisonment up to 2 years any person who by violating a protection or otherwise unjustified method gains access to a computer system or part of it.'

(23) It is stated in the preparatory works of the provision that 'the provision continues in effect the Penal Code of

1902, § 145, second paragraph, as far as it concerns data which is stored,' cf Ot.prp.nr.22 (2008-2009) page 403.

(24) This is deepened in the following way:

> 'This provision affects the very act that provides access to the computer system. Further use of the system, such as search and mapping of information contained on a computer, may be considered as illegal use. Modification or deletion of data and information found on the system, may be covered by the vandalism provisions.'

(25) The preparatory work emphasises that the perpetrator can only be punished if he has either violated a means of protection or has obtained access to all or part of the computer system in any other unauthorised manner, see page 403 of the bill:

> 'It is not a condition that the break-in occurs by breaking a protection, cf "or in any other unauthorised manner". Since violation of a protection is likely to be the most practical, this is however mentioned especially in the Act. The reservation regarding unlawfulness "unjustified" continued from Penal Code of 1902 § 145, second paragraph.'

(26) These preparatory works of a provision that is intended to have a content corresponding to § 145, second paragraph, must be given weight in the interpretation of this provision. I therefor find it correct to apply the interpretation of the law that is reflected in relation to the new provision, to the interpretation of § 145, second paragraph. It is on this basis it is clear that the defendant here received a password, and computer and access to inspect the machine in its entirety, which must mean that he has not gained unauthorised access to the data which after login lay open to him. He may, in my view, not be considered to have gained unauthorised access to information 'by other unauthorised practice'.

(27) The defendant had in addition to investigate the information that was stored on the PC, also installed a program on the computer, which enabled easy access to stored passwords, etc. The prosecutors have alleged that the defendant may nevertheless be punished for that part of the information which he acquired through the program.

(28) Counsel for the defendant has stated that the program enabled easy access to passwords etc for the defendant, but without enabling him through this to obtain access to areas of the computer that was password protected or protected in other way. It was fully possible to find the information without the program, at least for a computer-literate person. The prosecutor has not commented on this presentation. As this is the situation, I cannot see that any violation of § 145, second paragraph of the data were obtained using the search program.

(29) Another issue is that it is clear that A was not entitled to transfer the information to his own PC, but that is a different issue than comprised by the indictment.

(30) I have come to the conclusion that the defendant cannot be punished for violation of the Penal Code § 145, second paragraph under item I c, and that the appeal from the prosecution at this point must be rejected.

(31) *Whether the acquisition of data has occurred for gain, Penal Code § 145 subsection three*

(32) Penal Code § 145 subsection three raises the penalty when the accused has inflicted injury or acted with purpose of profit, and reads as follows:

> 'If harm is done by acquisition or use of such unwarranted knowledge, or the crime is committed for the purpose to obtain any improper gain, imprisonment for up to 2 years may be used.'

(33) The City Court with respect to all the factors in count I found the defendant acted with purpose of profit, and that harm was caused, and consequently that § 145 subsection three was applicable. The assessment that the data burglaries caused damages is not challenged, and I therefore find that § 145 subsection three shall apply to all counts – regardless of whether there is any purpose of profit or not.

(34) The Court of Appeal, outside of the appeal, considered the question of whether it was right that there was a purpose of profit, but agreed with the City Court that the defendant had had purpose of gain by the data burglaries covered by counts I a, b, d and e. Counsel for the defendant has argued that the interpretation of the law and the form of procedure by the High Court at this point is wrong.

(35) I cannot see how the Court of Appeal in considering whether the defendant acted with the purpose of profit has interpreted the law incorrectly. It is generally assumed that when a person without authority obtains goods with economic value for his own use, he profits

regardless of what kind of personal motive he or she has. Illustrative of this is Rt-1968-626, where the Supreme Court found that a defendant who had obtained womens wear for sexual motives, had acted for gain. The same should apply even if the owner – as in this case – is not deprived of any asset. The decisive factor must be whether the perpetrator unlawfully obtains an economic good, and not that the owner suffers a loss, see the comparison Rt 1975-473.

(36) By hacking i.e. of customer records, the defendant gained access to data regarding a vast number of people. The Court of Appeal has assumed that this mass of information has economic value, and that the defendant acted for gain in the performance of computer break-ins. This is in my view a correct application of the law.

(37) I find no reason to go further into the question of the defendant's copy of the private photographs that may be deemed to have occurred for the purpose of gain.

(38) *Can the defendant be convicted of a violation of the Personal Data Act?*

(39) The Court of Appeal found the defendant guilty on charges III and IV, which involved violation of the Personal Data Act § 48 subsection f, cf § 20 cf. § 19 and the Personal Data Act § 48 subsection a, cf § 31 first paragraph letter a and second paragraph. The offense was – in brief – that the defendant stored the personal information he had unlawfully gained access to, without informing those concerned about this and about who was the Data Controller, and without sending a notification to the Data Inspectorate.

(40) Both the prosecution and the defense have claimed acquittal on these counts. The prosecutor has stated that the provision to the indictment is directed towards the 'Data Controller' in the meaning of the law. The term is defined in § 2, paragraph 4 as 'the one who determines the purpose of the processing of personal data and the tools to be used.' In the view of the prosecution it is not natural to regard the defendant as a 'Data Controller' under the Act.

(41) Counsel for the defendant has agreed to this, and also argued that the defendant's actions must be regarded as 'processing of personal data carried out by an individual for merely personal or other private purposes,' which are exempt from the provisions of the law under § 3, second paragraph.

(42) The defendant had in this case unlawfully copied the personal data of millions of people and transferred the information to himself. The information was stored on his personal server, and according to the provided information, nobody else had access to it.

(43) I agree that the Personal Data Act does not apply in such a situation, and that the defendant cannot reasonably be viewed as 'Data controller' by law. Although the collection of data is beyond what may be considered normal personal activities, the definition and discussion of what is meant by 'Data Controller' and the delimitation in § 3, in my view shows that the defendant cannot be punished for violation of the mentioned provisions when the processing – as here – exclusively concerns clearly illegally collected and stored information.

(44) A consequently must be acquitted of violation of the Personal Data Act.

(45) *Sentencing*

(46) The defendant is convicted of four violations of Penal Code § 145 second cf first and third paragraphs, and for violation of the Copyright Act § 54 first paragraph letter b cf subsection three. It is the defendant's data break-in which causes the sentence in this case. It concerns serious computer crime, which has resulted in harm to the aggrieved in the form of loss of reputation to the companies and anxiety and discomfort to the individuals as a result of private information that has gone astray.

(47) The defendant was, in the Court of Appeal, sentenced to imprisonment for one year, nine months of which were suspended. He has now been acquitted for violation of the Personal Data Act, which does not have an effect on the sentence. The sentence set by the Court of Appeal is in my view not too strict.

(48) *Compensation for non-economic loss to the victims*

(49) Claims have been made by five of the aggrieved individuals in the case for damages for non-economic loss. The claims have been substantiated by the facts that the defendant unlawfully copied private information and intimate pictures of the victims or their closely related. For four of them this happened by the defendant entering their e-mail accounts and transferred attachments, etc to his own server. For the fifth victim this occurred when the defendant should have repaired her computer.

(50) A claim for non-economic loss requires a foundation in law, cf-1986-1326 at page 1344. The claims are here

made with reference to the Damages Compensation Act § 3-6, which reads:

> 'The person who has offended a person's honour and personal privacy, shall, if he has shown negligence or if conditions for sentence are present, pay compensation for the damage sustained and such compensation for loss of future earnings as the court, having regard to the degree of guilt and other conditions finds reasonable. He may also be ordered to pay such compensation (damages) for non economic loss as the court deems reasonable.'

(51) There is no doubt that the defendant obtained access to information of a private nature in the legal sense, and that he acted intentionally. Counsel for the defendant has referred to Penal Code § 390 and argued that it requires that the violation of privacy has occurred at 'public announcement' see definition in Penal Code § 7, paragraph 2 of the term 'public'. This is also referred to as the publication criteria. The defendant has not made public any private information, and demands for redress therefore depend on whether under § 3-6 is a requirement that the publication requirement in Penal Code § 390 is met. The provision reads:

> 'Anyone who violates the privacy by giving public notice of any personal or domestic circumstances will be subject to fines or imprisonment for up to 3 months.'

(52) I shall first look at the legislative history of the provision of redress. This originally appeared in the Penal Code Enforcement Act § 19 and authorised demands for redress inter alia when someone had committed libel against his better judgment according to Penal Code § 248. By Act of 10 March 1939, the right claims for redress extended to include violations of privacy according to Penal Code § 390. The authority to require redress for non economic damages were included in § 390, second paragraph, by reference to § 254, and it followed implicitly from the provisions that redress would be relevant where the violation had occurred in the public according to § 390.

(53) In 1958, the rules regarding redress were moved from criminal law back to the Penal Code Enforcement Act § 19a, cf act of 12 December 1958 No 1. The preparatory work specified that the conditions for claims for redress for non economic damages would be the same as before, cf Ot.prp.nr.5 (1958) page 8. But it was no longer following from the wording that a violation of § 390 was a condition for compensation.

(54) The rules regarding redress for non economic loss were then moved to the Act on torts § 3-6, and the provision in subsection got its present wording, cf Act of 25 May 1973 No 26. Once again it was made clear in the preparatory works that this did not involve any material change of rules, see Ot.prp.nr.4 (1972-1973).

(55) It follows from what I have said that the Act's history suggests that redress for non-economic loss for the infringement of privacy can only be sentenced when the publication requirement under § 390 is met. This is also how the provision has been interpreted in practice, cf-Rt 2006-799, where the Supreme Court discusses the condition of 'public communication' in section 46-50. Also in Rt-2010-258, the Supreme Court without further assumption based its decision on that redress for non economic loss presupposes that the infringement has taken place in a public notice under the Criminal Code § 390, see paragraph 43 of the judgment.

(56) The prosecutor has referred to statements in Rt-2008-489 Section 42 and Rt-2008-1089 paragraph 34, which seem to allow that the application of § 3-6 can be somewhat broader than what follows from Penal Code § 390. In these cases, however, it was clear that the information had been presented in public, and I cannot see that representations can be given emphasis here.

(57) The prosecutors have pointed out that article 8 ECHR on the right to respect for family and private life requires states to protect citizens against interference with the privacy by the authorities. The provision would also require measures to protect against interventions by other private entities or individuals, see the European Court (ECHR) judgment in Case ES against Sweden (Case 5786/08) (EMD 2008-5786) paragraph 57. The States' obligations under article 8 will normally be met if the wrongful act is punishable under national law, see ECHR judgment Stubbings and Others v the United Kingdom (Case 22083/93 and 22095/93 (EMD-1993-22083 and EMD-1993-22095)) paragraph 66. On this background I cannot see that the relationship to the ECHR constitutes crucial guidance for the case here.

(58) On this basis, it must be taken as a basis that unless otherwise required by the present Convention obligations of Norway, that claims for redress for non-economic damages for the infringement of privacy can only be imposed when the publication requirement of § 390 is met. The defendant's actions have not been published,

and the appeal against the High Court's judgment on this point must be rejected.

(59) I find reason to add that policy considerations in my view may suggest that § 3-6 should be able to apply for this type of violation of privacy, even if the violation has not been published. Many people currently have extensive private information stored electronically, and to find that unauthorised hacking into the e-mail accounts or obtaining access to other electronically stored personal information, will for most be experienced as a very unpleasant invasion of one's privacy. This is therefore an issue that could be the reason for the legislature to consider.

(60) *Claims for financial expenses from Photobucket Inc*

(61) Photobucket Inc is a U.S. company that offers online storage of digital images and videos. The defendant hacked into the company's customer database and gained access to the personal information of more than 66 million of its users. During efforts to uncover the relationship and pursue it in Norway, the company instructed engineer Svein Ingvar Willassen to go through the logs and other information in preparation for report of the crime to the police. Willassen invoiced 22,500 kroner to the company.

(62) Photobucket Inc in addition hired the lawyer Arve Føyen. He assisted the company in the matter and acted as a liaison to the police. Føyen invoiced Photobucket Inc 86,825 kroner for the work.

(63) Photobucket Inc presented a claim that the defendant had to cover the costs and expenses resulting from additional work caused to employees in connection with the discovery of and cleaning up after the data break in. The High Court accepted the claim with respect to payments to Willassen and Føyen, and awarded Photobucket Inc compensation totalling 109,325 kroner.

(64) The defendant has appealed the High Court decision regarding the claim for compensation. It is argued that it is the police who investigate criminal offenses, and that costs of private investigation is beyond what is protected by the law on torts. In the defendant's view, it is in reality legal costs, for which the aggrieved party is not entitled to reimbursement. Anyway, the size of the claim is unforeseeable.

(65) I have concluded that the appeal partially should be accepted. The rules regarding coverage of claims for compensation and reimbursement of litigation costs are different. The question is therefore whether the costs should be viewed as legal costs, see the Criminal Procedure Act § 439, or whether it is civil claims 'arising out of the same acts as the case concerns', see the Criminal Procedure Act § 3, and which are treated according to Chapter 29. If it is a question of legal costs related to the pursuit of the civil claim, the aggrieved party has basically no claim for reimbursement when the claim, as here, is presented by the prosecution, see Penal Code§ 439, second paragraph, cf Andenæs, Norwegian Criminal Procedure, 4th edition page 609.

(66) The boundary between the two types of claim is not clear. It is in theory supposed that costs incurred prior to the writ of summons to a certain degree may be classified as both legal costs and damages, cf Schei et al Sivil Procedures Act (2007) page 928.

(67) I find that in the present case is clear that the cost of engineer Willassen may be claimed as an ordinary tort claim. The cost of technical assistance was entirely incurred prior to the writ of summons and are of relatively modest size. As the Court of Appeal I assume find that it is foreseeable and natural for an American company which is exposed to hacking by a perpetrator in a foreign country, engages a data expert assistance in this country. This was necessary in order to clarify what had happened.

(68) Also, the bulk of the costs of legal assistance should be viewed the same way. Most of this work could be characterised as expenses incurred in direct connection with the review of the offense. I refer to the fact that it concerned a foreign aggrieved party and a type of crime that is difficult to reveal by the police without close cooperation with the aggrieved party. It was such a collaboration lawyer Føyen performed on behalf of victims. The expenses which were incurred by presenting a civil claim for compensation must be seen as legal costs. I find that Photobucket Inc judgment must be awarded 60,000 kroner of the legal expenses that involvement of lawyer Føyen meant for the company.

(69) This means that the defendant's appeal partially is upheld, and that compensation to Photobucket Inc reduced to 82,500 kroner.

(70) I vote for this.

Judgment:

In the Appeal Court judgement is made the following

changes:

1. A is acquitted of breach of the Personal Data Act § 48 subsection f, cf § 20 cf. § 19 and the Personal Data Act § 48 subsection a, cf § 31 first paragraph a, and second paragraph.

2. In compensation to Photobucket Inc A shall pay 82,500 – eighty two thousand five hundred – kroner within 2 – two – weeks from service of this judgment, in addition to the general interest for overdue payments according to the Act regarding interest on late payments § 3, first paragraph, first sentence from the end of the compliance deadline until payment is made.

(71) Judge Øie: I am in in agreement with the first justice for the substantial parts and in the decision.

(72) Judge Bårdsen: Likewise.

(73) Judge Bergsjø: Likewise.

(74) Justice Schei: Likewise.

(75) Following the voting, the Supreme Court made this judgment:

In the Appeal Court made the following changes:

1. A is acquitted of breach of the Personal Data Act § 48 subsection f, cf § 20 cf. § 19 and the Personal Data Act § 48 subsection a, cf § 31 first paragraph a, and second paragraph.

2. In compensation to Photobucket Inc A shall pay 82,500 – eighty two thousand five hundred – kroner within 2 – two – weeks from service of this judgment, in addition to the general interest for overdue payments according to the Act regarding interest on late payments § 3, first paragraph, first sentence from the end of the compliance deadline until payment is made.

With thanks to Arve Føyen for reviewing this translation.

