PrivacyStudio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 8
International Data Protection Laws

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Eight
INTERNATIONAL DATA PROTECTION LAWS

Companies operating in jurisdictions with comprehensive data protection laws must comply with procedural and substantive requirements of those laws. In Europe, for example, companies face regulatory action for failing to comply with process requirements (such as database registrations) or to respect substantive rights, such as providing individuals with access to their personal information. The following cases illustrate the types of actions commonly brought by data protection authorities.

Process Requirements

Many international data protection laws require data controllers to register their data processing activities with the national data protection authority. These registers provide both the regulators and the public with information about the types of data processing that occur and allow for transparency and corporate accountability. Failure to register can result in an enforcement action.

The United Kingdom's Information Commissioner stated in its 2005-2006 Annual report that in 2006 that it brought sixteen cases to enforce the Data Protection Act. Of these, eleven were based on the respondent's failure to register its data processing.

THE ABACUS RECRUITMENT CASE (AUGUST 2005)[142]

Respondent: Abacus Recruitment Services (Wales) Ltd.

Regulator: Information Commissioner (UK) (ICO)

Basis for Complaint: Violation of Data Protection Act 1998

Facts and Allegations: Despite being contacted by the ICO and informed that it must register its data processing activities under the Data Protection Act, Abacus Recruitment failed to register its data processing with the ICO.

Outcome: The ICO filed a claim against Abacus Recruitment with the Abergavenny Magistrates Court. The company was found guilty of the offense and ordered to pay a fine.

Fine Imposed: £2,000

THE DIFC REGISTRATION CASE (MAY 2007)[143]

Respondent: All Registered Dubai International Financial Centre Establishments

Regulator: Commissioner of Data Protection

Basis for Complaint: Data Protection Law. DIFC Law No. 1 of 2007

Facts and Outcome: The Commissioner issued an Enforcement and Compliance Notice to all registered DIFC entities regarding Article 25 of the Data Protection Law (the Law) and the published Data Protection Regulations. The notice stated that:

(1) The law was in full force and effect;

(2) All DIFC entities (regulated and unregulated) must register with the Commissioner no later than June30, 2007;

(3) Entities previously registered (under the 2004 law) must register under the Law by June 30, 2007; and

(4) Entities that do not comply will be subject to fines and penalties.

Fine Imposed: None

Limits on Data Collection

Data protection laws typically limit a data controller's ability to collect personal information. Controllers should only collect information that is reasonably needed to accomplish the purpose for which the information is being collected; companies should not collect excessive data. Overbroad collection attempts can lead to complaints and data protection authority actions.

THE INSURANCE CONSENT FORM CASE (JANUARY 2007)[144]

Respondent: Canadian Insurance Adjuster

Regulator: Office of the Privacy Commissioner of Canada

Basis for Complaint: Violation of the Personal Information Protection and Electronic Documents Act (PIPEDA)

Facts and Allegations: A complaint was filed by consumers with the Privacy Commissioner's Office regarding overboard data collection efforts by a Canadian insurance adjuster. The consumer alleged that when he reported the theft of personal property to his insurance company, he was required by the adjuster to sign a Personal Information Consent form.

The consent form provided that personal information could be obtained by the insurance adjuster to determine the value of the loss, to determine available coverage and to prevent fraud. The form listed seven types of personal information that could be obtained by the adjuster:

- Basic identifying information
- Claims and credit history
- Financial information
- Medical information
- Driver's record
- Employment information

- Witness statements

According to the consent form, this information could be collected from credit organizations, motor vehicle and driver licensing authorities, financial institutions, medical professionals, fire/intrusion protection system installers and monitoring companies, and various police and other authorities. The form also listed nine categories of third parties to whom the personal information may be disclosed.

As the individual was making a claim related to the theft of personal property, he objected to the requirement that he consent to the collection of information such as his credit history, financial information, medical information, driver's record, and employment information. However, when he refused to sign the form, the adjuster indicated that the claim could not be processed and would be denied. The Privacy Commissioner investigated the matter and concluded that his complaint was well-founded.

In making this determination, the Commissioner noted that PIPEDA "Principle 4.3.3 states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes. Principle 4.4.1 stipulates that organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices."

Outcome: After discussing the complainant's concerns with the adjuster, the adjuster agreed that this consent language did not meet the requirements of Principles 4.3.3 and 4.4.1. The adjuster agreed to waive the requirement that the complainant sign the Personal Information Consent form. It also agreed to redraft the language of the form to comply with the requirements of PIPEDA.

The Privacy Commissioner's Office also learned that the Personal Information Consent form was an industry standard form, drafted by an insurance industry association. The Privacy Commissioner's Office therefore raised the matter with the Canadian Independent Adjusters' Association and the Insurance Brokers Association of Canada. These associations agreed to revise their consent forms to comply with PIPEDA and to ensure that members were using the new forms.

Fine Imposed: None

THE COUPON INFORMATION CASE (SEPTEMBER 2007)[145]

Respondent: A Hong Kong credit company

Regulator: Privacy Commissioner for Personal Data ("PCPD")

Basis for Complaint: Violation of Data Protection Principle 1 (DPP1) of the Hong Kong Personal Data (Privacy) Ordinance

Facts and Allegations: A citizen received a letter from a credit company in Hong Kong in early January 2006. A form was enclosed in the letter, stating that the receiver could get supermarket gift coupons if "simple information" was provided on or before a specified date on a form. According to the instructions on the form, an applicant was required to provide name, sex, Hong Kong Identity Card Number, correspondence address, email address (optional), telephone number, name of employing company, position category, and age and income

groups, and then fax or post the form to the credit company. Upon verification, the applicant would be offered a supermarket gift coupon of HK$20.

The citizen enquired if such activity had contravened any requirement of the Ordinance. Although the citizen had not formally lodged a complaint, the PCPD initiated an independent investigation of the credit company.

The PCPD concluded that DPP1 in Schedule 1 to the Ordinance and paragraph 2.3 of the Code of Practice on the Identity Card Number and other Personal Identifiers ("the Code") issued by the Commissioner under section 12 of the Ordinance were relevant to this case.

DPP1(1) provides that: *"Personal data shall not be collected unless- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data; (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and (c) the data are adequate but not excessive in relation to that purpose."* Additionally, the Code provides strict limits on the collection and use of the national Identity Card Number.

Outcome: In conducting its investigation, the PCPD accepted the company's arguments that the information required on the form, with the exception of the Identity Card Number and name of the applicant's employer, were relevant to the promotional offer and not excessive. The PCPD wrote:

> *In my opinion, to achieve the purpose of [the] promotion, it is necessary for the credit company to contact the relevant persons. Therefore, the collection of the name and contact information of the applicants is necessary. Regarding the information on sex, age, position and income, etc., I agree that such data are helpful to the promoter in understanding the background of the target customers so that appropriate services or products can be chosen for promotion to increase the chance of success. Moreover, I notice that the credit company has adopted a less privacy intrusive alternative when collecting such background information, i.e. no collection of the actual age and income amount, but only the age and income groups. In the circumstances of the case, I am of the view that the collection of the name, correspondence address, telephone number, sex and information on age, position and income groups of the applicants for promotion purpose is not excessive, and thus there is no contravention of DDP1(1) of the Ordinance.*

With regard to the Identity Card Number, the PCPD reached a different conclusion:

> *I do not accept the credit company's explanation that the collection of ID card number of the applicants was necessary. On the contrary, I think it can adopt other feasible and less privacy intrusive alternatives to substitute for the collection of ID card number. Therefore, I am of the view that the credit company had contravened the requirement in paragraph 2.3 of the Code. As the credit company was not able to provide any evidence to prove its compliance with the Ordinance by other means, I consider that the collection of ID card number of the applicants for the said purposes by the credit company was excessive, and DDP1(1) was contravened.*

Similarly, the PCPD found that collection of the applicant's employer's name was excessive.

The credit company agreed to delete the excessive data from its databases. It also agreed to cease collection of these data elements in its promotional forms going forward.

Fine Imposed: None.

Respecting individual Rights

International data protection laws generally require data controllers to respect consumer rights of access, correction and deletion. Data protection authorities use their enforcement powers to defend consumers whose rights have not been respected.

THE JEWELRY STORE MAILING LIST CASE (JANUARY 2005)[146]

Respondent: A Jewelry Store

Regulator: Hellenic Republic Data Protection Authority

Basis for Complaint: Violation of the Greek Data Protection Law (Law 2472/1997)

Facts and Allegations: The Greek DPA received a complaint from an individual that a jeweler had mailed the individual a greeting card [*apparently a marketing communication*], despite his never having transacted business with the store. Upon receiving the communication, the individual had contacted the jeweler and requested information about the personal data held by the jeweler and the source of the data. The jeweler vaguely responded on the phone that it had obtained information about members of a certain club, but the individual had not been a member of that club. The jeweler refused to provide more information and did not respond to the individual in writing.

Article 12 § 1 of the Greek data protection law provides that "Everyone is entitled to know whether personal data relating to him are being processed or have been processed. As to this the Controller must answer in writing…" Individuals are also entitled to know the source of data provided about them pursuant to Article 12 § 2a. Should an entity not respond to an access request within 15 days, the law provides that an individual may appeal to the DPA. The DPA may issue administrative sanctions to enforce compliance.

Outcome: The Greek DPA investigated the complaint and concluded that the jeweler had contravened the data protection law.

Fine Imposed: €3,000

THE ASHBURY TAVERNS CASE (2006)[147]

Respondent: Ashbury Taverns

Regulator: Data Protection Commissioner – Ireland

Basis for Complaint: Violation of Data Protection Acts 1998 & 2003

Facts and Allegations: The Commissioner's office received a complaint regarding alleged non-compliance with an access request. This complaint was made by a legal representative on behalf of a data subject formerly employed by Ashbury Taverns of Wexford.

When the Commissioner's Office did not receive a response to its inquiry, it issued an Enforcement Notice requiring Ashbury Tavern to comply with the access request within a period of twenty-one days.

Outcome: Ashbury Tavern, through its lawyers, responded to the Enforcement Notice and provided the individual with access to the requested data.

Fine Imposed: None

In its 2006 Annual Report, the Irish Data Protection Commissioner emphasized the importance of access rights,[148] noting that complaints about data controllers failing to provide access constituted the second largest category of complaints in 2006 (following only by complaints about electronic communications, such as telemarketing and email), the Commissioner wrote:

> *The right of access to personal data is a fundamental right that is enshrined in data protection legislation. I have the power to take immediate action to vindicate this fundamental right of a data subject. In response to the increase in the number of complaints received in relation to such requests, following a review, we have radically altered our approach to resolving these complaints to better serve the interests of data subjects.* ***The emphasis now is on enforcement.***
>
> *Data controllers who fail to inform the data subject of the reasons for refusing an access request contravene Section 4(7) of the Acts. Under the new procedures, data controllers who appear to be breaking the law in this way are given ten days from the start of my investigation to inform the data subject in writing (and to copy the correspondence to my Office) of the provisions of the Acts which s/he is relying on to withhold the personal data or, if he/she has no provisions to rely on, to comply with the access request immediately.*
>
> *The data controller is informed that if, within the ten days, the access request is not complied with, I will commence enforcement proceedings fourteen days from the start of my investigation. I will not take such action in the rare case where the data controller can demonstrate that access can be denied under one of the exceptions provided for in the Acts. Failure to comply with an Enforcement Notice is an offence liable to a fine on summary conviction in the District Court of €3,000.*
>
> *I am confident that the new strategy which I have put in place will help considerably to enforce the legitimate rights of data subjects who have suffered a violation of their access rights at the hands of what are usually ill-informed but sometimes deliberately evasive data controllers. Data controllers in such situations should be aware that my enforcement powers have real teeth and I will have no hesitation in applying those powers in their direction. Furthermore, in the interests of vindicating this fundamental right of data subjects, I am not in a position to tolerate efforts by such data controllers to delay my investigations through the raising of spurious legal issues.*
>
> *Under new procedures, the commissioner said, data controllers who appear to be in contravention of the data protection acts "are given ten days from the start of my investigation to inform the data subject ... of the provisions of the Acts which s/he is relying on to withhold the personal data, or, if s/he has no provisions to rely on, to comply with the access request immediately.*[149] *(emphasis above in the original)*

Additionally, although these cases address access rights under international data protection laws, it is important to consider that many United States privacy laws also provide individuals with rights of access. For example, the Fair Credit Reporting Act and the HIPAA Privacy Rule both contain strong consumer access provisions. The Children's Online Privacy Protection Act provides parents with a

right of access to information stored about their children. United States regulators such as the Federal Trade Commission and the HHS Office of Civil Rights rigorously enforce these obligations.

THE T-ONLINE CASE (2006)[150]

Respondent: T-Online, a German Internet Services Provider

Regulator: [Court decision] *Party Names Withheld by Law,* BGH, No. BGH III ZR 40/06, 10/26/06, upholding a decision by the Municipal Court of Darmstadt (300 C 397/04)

Basis for Complaint: Inappropriate data retention; refusal to comply with deletion request

Facts and Allegations: Holger Voss, a T-Online customer, filed an action against T-Online, based on the ISP's refusal to delete certain Internet protocol (IP) logs. T-Online claimed that the logs were needed to track Internet usage for billing purposes. However, Voss paid T-Online a flat fee for Internet access, so his usage was not relevant for billing purposes.

In ruling for Voss, the municipal court said that: "[s]aving the user data is not justifiable," and "if one were to accept [T-Online's] argument, then one could also allow the storage of information about individual websites visited ... another way to document a person's Internet usage. Even saving the contents of files could be justified with [T-Online's] argument."

Outcome: As a result of the ruling, T-Online must comply with certain consumer requests to have IP log data deleted.

Fine Imposed: None

Additionally, to further protect individuals, European data protections limit the ability of a data controller to transfer personal information to recipients in other countries unless adequate protection for the personal information is assured. Other countries that restrict data transfers include Argentina, the Dubai International Financial Centre, and some Canadian provinces.

THE TYCO HEALTHCARE CASE (APRIL 2007)[151]

Respondent: Tyco Healthcare France

Regulator: Commission nationale de l'informatique et des libertés (CNIL)

Basis for Complaint: Inappropriate data retention; refusal to comply with deletion request

Facts and Allegations: In 2004, Tyco Healthcare France registered a database with the CNIL. The registration filing indicated that the database contained non-sensitive information of the companies' 450 workers. It was used for internal management purposes and for reporting to the French company's US parent. At some point, the CNIL asked Tyco to provide additional information about the purpose for the database as well as information on the cross-border transfers of the employee information. The company responded by telling the CNIL that it had discontinued use of the database.

In 2006, the CNIL conducted an inspection of Tyco Healthcare France and discovered that the database was still in use. Additionally, the database contained many data elements that had not been listed in the initial registration, including "salary history, aptitude and willingness to undertake missions requiring international mobility, stock option attributions and status, participation in training activity, and other internal evaluations." The personal information was also transferred internationally, and resided on corporate computer servers in the US.

Outcome: The CNIL issued sanctions against Tyco Healthcare France and published a written warning regarding non-compliance with French database registration requirements and cross-border transfer rules. These rules apply to all data transfers, even those within a corporate family.

The CNIL also reminded companies generally that French employees have rights of access to all personal information stored in such databases, including performance review data, evaluations, and ratings of potential.

Fine Imposed: €30,000

Management of Data Processors

International data protection laws also require companies to manage third party processors. For example, **Article 17 of the EU Data Protection Directive** requires data owners (controllers) to choose processors that can provide "sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out" and to ensure compliance with those measures. The Article goes on to require that processing performed by a third party data processor must be governed by a written contract or legal act binding the processor to the controller and stipulating that (1) the processor shall act only on instructions from the controller, and (2) the security measures described above shall be met.

Data protection authorities have also published regulations as guidance on the management of third party data processors.[152] These instructions focus generally on vendor qualification, contracting, oversight, and security. Failure to comply with these instructions can lead to regulatory actions.

THE MARKS & SPENCER CASE (JANUARY 2008)[153]

Respondent: Marks & Spencer PLC

Regulator: Information Commissioner (UK) (ICO)

Basis for Complaint: Violation of Data Protection Act 1998

Facts and Allegations: Marks & Spencer (M&S) is a UK retailer, and a data controller under the UK Data Protection Act. M&S employed an independent data processor to prepare statements for members to its company pension scheme. To complete this task, the data processing company was provided with personal information about the pension plan members. A company principal downloaded the data to a laptop computer, which was later stolen from his home.

The Data Protection Act provides that: "*Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller must… (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 11 of Part II of Schedule 1 of the Act)

After investigating the matter, the ICO concluded that M&S violated the Data Protection Act by failing to take appropriate measures to secure the personal information. In particular, the ICO alleged that M&S should have required its data processor to encrypt the personal information on the laptop. Given the possible risks of harm ("damage and distress") that may be caused as a result of the breach, the ICO chose to file a formal enforcement notice against M&S.

Outcome: The ICO issued a formal Enforcement Notice against M&S. This Notice requires M&S to ensure that personal data are processed in accordance with the Act and, in particular, ensure that the process of laptop hard drive encryption commenced by the data controller in October 2007 is completed by 1 April 2008

Fine Imposed: None

Similarly, Dr. Omer Tene reports that the Israeli data protection authority has brought an enforcement action when an agency failed to control its data processors:[154]

> *In September 2007, Israeli Law and Information Technologies Authority ordered the Ministry of Defense and its contractor, Pemi Premium Co., to stop using a database, which held medical data concerning disabled army veterans. The order came after a compliance audit held at Pemi Premium, which determined that sensitive medical data were not adequately secured. In addition, ILITA found that Pemi Premium failed to comply with Ministry of Defense guidelines specified in the outsourcing contract. For example, the company did not administer reliability tests for employees handling the data and transferred data to third parties without informing the Ministry of Defense.*

While liability for processor misdeeds generally falls on the data controller, processors themselves face liability for handling personal information in ways that are contrary to the processing contracts.

According to a March 2005 BNA Privacy Law Watch story,[155] a German data processor was investigated by the Hessen data privacy commissioner. In this case, Systemform Mediacard GmbH and its affiliate GHP Document Services GmbH provided a Vietnamese subsidiary with copies of information on patients of a Hessen state health insurance firm. The copies were provided so the subsidiary could test new document scanning software. In bringing the complaint, the insurance firm noted that its contract prohibited any unapproved transfers of patient information. Although no abuse of the patient data occurred, the Schleswig-Holstein data privacy commission, commenting for the BNA story, indicated that the transfer of the patient data to Vietnam was a "scandal" and noted that the processor had jeopardized its contracts with the insurance firm.

In Japan, BB Technology, an internet service provider, was found liable certain Yahoo! BB customers whose personal information was misappropriated as a result of the sharing of a username and password

by former employees of BB Technology's predecessor (Softbank BB).[156] The username and password was used to access the personal information of at least 4.6 million Yahoo! BB customers. A group of these customers sued Yahoo! BB and BB Technology in the Osaka District Court, seeking compensation for the emotional distress suffered as a result of the incident. The Court found that BB Technology had breached its duty of care by not having appropriate security controls and awarded 6,000 yen to each of the plaintiffs. The Court rejected the claim against Yahoo! BB, finding that it did not breach an obligation to supervise BB Technology.[157]

In the United States, both HIPAA and the Gramm-Leach-Bliley Act require mandate appropriate due diligence of and contractual controls on service providers. Some states, including California, also require appropriate oversight of data processors.