## SELLING A COPY OF A CUSTOMER LIST WITHOUT PERMISSION NOT A CRIME!

**When an employee of TNT Roadfreight (UK) Ltd. recently tried to sell a copy of his company's marketing list to a competitor, he could hardly realize that he would be prosecuted. Even worse, that his case would raise fundamental problems affecting interpretation of the Council of Europe's Recommendation on the Protection of Personal Data Used for the Purposes of Direct Marketing (see box), the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), Scottish criminal law and wider common law.**

+ In terms of the Recommendation on Direct Marketing, his case touched on the clauses on making available name-linked lists to third parties and data security.

+ In terms of the OECD Guidelines, the issue was one of reasonable security safeguards, a principle which in the Guidelines extends to manual (non-computer) records.

+ In terms of Scottish criminal and wider common law the issues were these:

1. Is selling a copy of a company's customer file, without permission, a crime?

2. If not, can a court declare that such conduct is in effect a crime in any case?

Rather surprisingly, in June, Scotland's supreme criminal court said no to both of these questions.

---

### THE COUNCIL OF EUROPE RECOMMENDATION ON DIRECT MARKETING

The Council of Europe's Recommendation on Direct Marketing, adopted in October 1985, offers a common set of principles to guide companies, legislators and data protection authorities on how to apply data protection principles to the use of marketing lists. The Recommendation covers:

* the collection of data,
* safeguards for sensitive data,
* the making available of lists to third parties,
* the rights of the data subject (like the right to gain access and to correct data),
* the presentation of marketing messages and material, and
* data security

---

**David Goldberg of Glasgow University analyses the issues arising from this case.**

The vexed problem of how to fit the communication of information into a secure legal framework has now occurred in several countries and in June this year confronted Scotland's High Court of Justiciary, Scotland's supreme criminal court. (Scotland's legal system is separate from that of England and Wales). The novelty of this case (Grant v. Procurator Fiscal, Edinburgh) was that the charge was not based on any statute, as in the English case of Oxford v. Moss ([1979] 68 Cr.App.R. 183) or in the Canadian case of R. V. Stewart (149 D.L.R. 3rd Edition 583) for which the appeal to Canada's Federal Supreme Court will be heard later this year. Instead, the prosecutor proceeded on the basis of the common law. The argument was over:

* whether or not attempting to sell the information on a company's customer list constituted a crime, or

* if it were not, whether the Court should declare such conduct to be criminal (there is a residual power in the court to declare obviously unlawful "novel" conduct to be criminal).

**The Facts**

The facts of the case were that a transport services company, TNT Roadfreight (UK) Ltd, kept lists of its customers and its dealings with them on its computer. Grant, an employee, was authorized to have access to these records and as a salesman kept the printouts at an office away from the computer site. Grant made a copy of the customer list (not using his company's copier) with the intention of selling it. Grant telephoned the manager of Edinburgh Distribution Services, a company in competition with TNT Roadfreight, and at a meeting offered to sell to the competitor a copy of TNT's customer list for £400.

**The Decision**

The court held that:

1. such conduct did not fit into any existing category of crime known to Scots law, even though the judge described Grant's conduct as "dishonest exploitation of confidential information," and that

2. although immoral and reprehensible, the conduct should not be declared a crime.

As Lord Macdonald said, for the court to declare that it is a crime "dishonestly to exploit confidential information belonging to another would have far reaching consequences in this technological age."

**Commentary**

This case indicates how difficult it is - both from an operational and a legal point of view - to classify information, and to cope with the various ways of trading in it. There are two main aspects:

1. the options available to TNT Roadfreight against Grant's conduct, and

2. the views taken by any of TNT's customers, whose names and business relationships are contained in the printout and who may object to such details being communicated to a third party.

**TNT Negligent?.....**

Could, for example, any action in negligence lie against TNT Roadfreight in such a case, if it were shown that TNT had failed to take "reasonable security safeguards," in the words of the OECD Guidelines' fifth principle? This states that, "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." In the Guidelines' official explanation, unauthorized "use" is interpreted as "unauthorized copying," which would clearly apply to the TNT case. Any system of booking out printouts would probably avoid such an action for civil damages, but it cannot prevent the further communication of the information, whether orally or by way of a copy. Perhaps such exposure of a name on the customer list would amount to an unjustifiable invasion of privacy? Again, much will depend on whether the data system offered a reasonable and appropriate level of security for the data and the extent to which privacy claims were recognized by a court.

**....or a civil claim against Grant?**

The High Court of Justiciary was clear that TNT Roadfreight had a good civil claim, in principle, against Grant, as Grant had broken his explicit or implicit obligation of confidence under his contract of employment not to release his employer's confidential information. But what remedy should the company seek?

1. Seeking a legal ban is too late. TNT had no prior knowledge of Grant's attempt to communicate the information to a third party,

2. Damages depend upon showing some loss. At the time of the attempted sale of the customer list, no loss could be shown,

3. Even if the list were sold, quantifying the loss resulting from the exchange of information would be very difficult.

The difficulty that confronted the court, and led it to recommend reform of the law by parliament was that, "it would be very difficult to define the new crime in such a way that it could clearly be applied in other cases." A particular problem for the court was their appreciation of other ways of doing the same sort of thing. I suggest that these could include the following:

* An employee copies the data on the computer site using his own writing materials, and sells the data to another party.

* An employee memorizes the data, writes it down later (or on several occasions) and sells it to another party.

* An employee memorizes the data and transmits all or a part of it to another

party verbally for a fee.

* An employee does any of the above, not for a fee but for another

benefit, such as being given a job by the other party.

* An employee becomes familiar with the information on the customer list just by doing his job, leaves his employer by mutual agreement, is later employed by another company and uses the information in the course of his new job.

* An employee does any of the above, leaves his employer by mutual agreement, and becomes self-employed, and makes use of the data in his own business.

**In which of the above cases is the employee "dishonest?"**

The Scottish Law Commission in its Report on Breach of Confidence (No. 90, 1984, page 53) considers the sanction of "exemplary damages" (as a warning to others) in cases where confidential information had been "stolen or obtained without authority." This approach is rejected as "very much out of keeping with the general principles underlying the Scottish remedies in contract" and civil damages.

So it is now clear that the position for companies in Scotland is exposed in cases where an employee sells a customer list or other commercially valuable name-linked data. No obvious or clear legal analysis of the situation exists, no remedy is available, nor procedure is practical beyond existing security instructions, which, of course, rely on the goodwill of the recipients. However, even a negative result clarifies the situation. A positive resolution of this legal uncertainty will have to await until the UK Parliament finds time to legislate.

David J.A. Goldberg, Lecturer, School of Law, University of Glasgow; and Consultant in Information Law.

**Note: David Goldberg suspects that his comments on this Scottish case apply generally to other common law countries. Would any readers who have information on any similar cases in either common law or other countries please contact us at PL&B? We would be happy to report on this evolving issue where data protection is closely linked with other branches of the law.**