Issues in the Emerging Law of Information.

HORACE KREVER

No matter how one defines it, law is a stabilizing force in society. It is therefore to be expected that in an era of rapid technological advances, changes in the law will be slower than changes in technology. To put the matter another way, changes in technology create changes in relationships between members of society, between institutions and between members of society and institutions that the law, or perhaps more accurately, lawmakers, that is, legislatures and judges, could not foresee or even contemplate. This phenomenon, at any given time, results in the weakness of the law as an instrument to adjust or reconcile the changing and conflicting interests. It creates a need for speedier law reform.

But law reform as it relates to tehnological developments must be brought about thoughtfully and with a view to avoiding simple solutions to an immediate problem, solutions which, in the long run and as technology continues its relentless progress, will result in even greater problems as time advances.

In the next few minutes I want to illustrate the difficulty I am trying to describe by considering two legal approaches to information and the transmission of information which, given their value and speed, the law can be forgiven for failing to contemplate when current theories of liability were formulated. I have in mind the question of the nature of information, including computerized information. This question was the subject of a recent decision of our highest court, the Supreme Court of Canada, as recently as May, 1988. The answer which it gave in Stewart v. The Queen (1988), 41 C.C.C. (3d) 481, was an answer for the purpose of the criminal law only, that is for the purposes of culpability for which punishment might be imposed. Although the answer was in negative rather than positive terms, we at least learned what information - confidential information - is not. It is not something that can be stolen or in legal terms, it cannot be the subject of theft. The court was conscious of the possibility that this state of the law may not meet the needs of a contemporary information-driven society. But if reform is needed the reform should not be brought about by the courts in the context of a prosecution for the criminal offence of theft. Speaking for a unanimous court, Mr.

Justice Lamer said (at p. 492):

> I am of the view that, given recent technological developments, confidential information, and in some instances, information of a commercial value, is in some need of protection through our criminal law. Be that as it may, in my opinion, the extent to which this should be done and the manner in which it should be done are best left to be determined by Parliament rather than by the courts.

The case was one involving a charge of counselling theft. An employee was asked to obtain the names, addresses and telephone numbers of his employer's employees. It was known that this information was confidential and a price was to be paid for each name. The employee was not to take the documents containing the information. As Mr. Justice Lamer put it:

> We are not here dealing with the theft of a list or any other tangible object containing confidential information, but with the theft of confidential information per se, a pure intangible.

The Criminal Code of Canada defined theft in s. 283(1): (now s.322(1))

> Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate, with intent
>
> a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it;
>
> d) to deal with it in such manner that it cannot be restored in the condition in which it was at the time it was taken or converted.
> (underlining added for emphasis)

The Court had to decide what the meaning of "anything" in the subsection I have just read means. It held that the language of the subsection restricts the word "anything" in two ways:

> (1) whether tangible or intangible, "anything" must be of a nature such that it can be the subject of a proprietary right, and
>
> (2) the property must be capable of being taken or converted in a manner that results in the deprivation of the victim.

The way in which civil cases have dealt with confidential information was thought not to be relevant. And as to the danger of changing the law to deal with an immediate problem this advice was given:

> The criminalization of certain types of conduct should not be done lightly. If the unauthorized appropriation of confidental information becomes a criminal offence, there would be far-reaching consequences that the courts are not in a position to contemplate.

Moreover, said the court, in the case of confidential information the taking or converting, or appropriation does not in any way deprive the owner of his, her or its proprietary interest. Recognizing that the judgment was one of policy, Mr. Justice Lamer summarized the reasoning leading to the policy decision as follows: (pp. 495-6)

> To summarize in a schematic way: "anything" is not restricted to tangibles, but includes intangibles. To be the subject of theft it must, however:
>
> 1. be property of some sort;
>
> 2. (a) taken - therefore intangibles are excluded; or
>
> (b) converted - and may be an intangible;

(c) taken or converted in a way that deprives the owner of his proprietary interest in some way.

Confidential information should not be, for policy reasons, considered as property by the courts for the purposes of the law of theft. In any event, were it considered such, it is not capable of being taken as only tangibles can be taken. It cannot be converted, not because it is an intangible, but because, save very exceptional far-fetched circumstances, the owner would never be deprived of it.

For all these reasons, I am of the opinion that confidential information does not come within the meaning of the word "anything" of s. 283(1) of the Criminal Code.

So much, for the moment, for our criminal law. To what extent is there satisfactory protection of confidential information in our civil law? In my opinion, not enough. This opinion resulted from an extensive Royal Commission Inquiry into the Confidentiality of Health Information in Ontario which I had the honour to conduct. I reported in December, 1980. The report documents the real risks to which confidential information, both computerized and manual, are constantly exposed. For present purposes it is probably enough to state the following conclusions the evidence established:

1) Confidential health information is not secure or perhaps more accurately put, the confidentiality of information required by law to be kept confidential, is not secure.

2) Confidential health information - probably all confidential information - has a commercial value.

3) Persons whose confidentiality is invaded by unauthorized access to the information often suffer a loss or real harm, and

4) Current civil law does not provide an adequate or, in some cases, any remedy to the person injured by a breach of his or

her confidentiality.

Not only is the injured person left without a satisfactory remedy but, and this may be the other side of the coin, there exists no satisfactory sanction to deter would-be invaders from invading confidentiality. We have seen that there is no criminal-law sanction. What is wrong with the tort-law sanction? A good deal. The weaknesses and the potential of traditional common-law remedies for unwarranted disclosures of personal information are very well analyzed by Professor Sanda Rogers of the University of Ottawa's Faculty of Law in her essay, Common Law Remedies for Disclosure of Confidential Medical Information in Issues in Tort Law (Toronto, The Carwsell Company Limited, 1983) a collection of essays, edited by Professors Steel and Rodgers. Of the defects in the tort remedy discussed in the essay, to my mind the most serious one relates to the high cost of litigation when contrasted with the actual damages a plantiff can show he or she has suffered as a result of the unauthorized disclosure. Professor Rodgers concluded her essay with these observations at p. 298:

> Two major drawbacks to private litigation as a deterrent device in this domain must be mentioned. As the Krever Inquiry made clear, confidential medical information is a valuable commodity. Therefore, except where disclosure is authorized by the subject or by law, measures to deter unwarranted disclosure must be designed with sufficient effect so at to outweigh the economic attraction of participating in such disclosure.
>
> Private litigation by the subject of any disclosure is hardly the optimal mechanism of deterrence for two reasons. Firstly, the subject of an unwarranted and unauthorized disclosure is unlikely to know, in the great majority of cases, that such disclosure has occurred. Secondly, even where the subject becomes aware that disclosure has taken place, the nature of the damages may well be such as to fall within the domain of damages poorly compensated, or simply not compensated, by the law. Even where compensable, the costs of a private action to so recover are likely to make such an action uneconomic. Rather, thought must be given to legislative control of abuses in this domain.

I agree. In my report I said this. (Vol. I,. p.530):

> [P]rivate litigation has two serious shortcomings. First, in the great majority of cases, the subject of an unwarranted and unauthorized disclosure is unlikely to know about the disclosure. Second, even if the subject learns about the disclosure, the measure of damages may well be so low that a civil action would not make economic sense. Nevertheless, I have reached the conclusion that the law should permit patients to commence an action for damages for the unauthorized, unjustified disclosure of their health information to third persons or for the inducing of such a disclosure.
>
> These drawbacks of private litigation may be overcome by creating a right of action without the need to prove actual damage. Damages should be presumed in a significant amount, say $10,000.00. The creation of a statutory cause of action would surely act as a deterrent. Those who might contemplate releasing or attempting to obtain health information without authorization and in unjustified circumstances should have to weigh the risk of judgment in this sum against the value of the information. Moreover, it would justify the patient in resorting to law. Finally, and perhaps most important, a statutory right of action would be a significant symbol of the value our society attaches to the right of privacy.

The precise words of the recommendation are these:

> 13. That a statutory right be created permitting a patient whose health information has been disclosed without his or her authorization, to maintain a civil action for the greater of his or her actual damages or $10,000.00 against:
>
> (a) any health-care provider or other person under an obligation to keep health information about the patient confidential, who unjustifiably

discloses his or her health information to a third person; and

(b) any person who induced anyone under an obligation to keep health information about a patient confidential, unjustifiably to disclose his or her health information.

That was 1980. In the last sentence of her essay, written in 1983, Professor Rodgers said: "The time has come to implement the recommendations of the ... Inquiry and to provide for a special statutory right of action. This seminar has demonstrated how speedily technological advances occur. It is not surprising, then, that the law will inevitably lag behind technology. But when does a time-lag become unreasonable?

***

August, 1989.