PRIVACY AND THE LAW

by

HARRY STREET

Dunning Trust Lecture 1969
Queen's University
at Kingston, Ontario

An offprint from
QUEEN'S QUARTERLY
LXXVII, No. 3
Autumn, 1970

*Privacy and the Law**

by

HARRY STREET

A noted British jurist here examines the actual or potential violations of personal privacy that accompany advances in technology, exposes the present inadequacies of the law in combatting such abuses, and suggests urgently needed measures to give legal protection to the individual in this area of civil rights.

NOW more than ever before, all countries seem to be confronted with the same new and urgent legal problems at one time. For example, we all are concerned now with how to compensate the victims of road traffic accidents, how to control medical transplants and how to regulate pollution. The reasons for this are obvious. The pressing issues these days are created by technological devices, or by business methods which rapidly spread around the world, whether they originate in Africa, America or Europe. Fortunately there has been a counterbalancing international realization of the homogeneity of these problems, a free communication between countries and a mutual cooperative search for the right answers. The further characteristics of these new issues is that they are not ones for lawyers only; they demand also the combined efforts of the political and applied scientists. Nor are they fully international in that one and the same answer will not be appropriate for every state.

All of this is true of the topic of this paper — Privacy. It was of no importance in the last century simply because business methods did not assail it, and there were no inventions the use of which interfered with it. It is now a pressing problem because of changed business practices and the widespread manufacture of new kinds of mechanical devices. International conferences are being held, governmental law reform commissions have it high on their agen-

* Dunning Trust Lecture delivered at Queen's University, 7 January 1970, in the series, "Freedom and Responsibility in Contemporary Society."

das, legislatures debate it, and articles appear in the press and learned periodicals. Lawyers are not so conceited or blind as to think that they can provide the answers unaided. We need guidance on public opinion, especially on what interferences citizens are willing to tolerate. The scientists must tell us the actual and potential range of their instruments and the medical profession must advise us on the possible psychological and physiological effects.

Most issues of civil rights are a confrontation between government and citizen, fewer between business and the individual. Privacy is double-headed: man is menaced by the executive and private enterprise alike. This erects further obstacles if legislative reform is sought: governmental interest in the *status quo* supported by business pressure groups does not make for the rapid enactment of new statutes. Many current legal problems call for simple answers. Shall the damages awarded to personal injury victims be reduced if they are at fault; shall owners of animals be liable for harm even though they are not negligent? There is no such legal purity about this problem. There is much more to it than whether those whose privacy is attacked shall be compensated after the event in a court action for tort. We must face problems of criminal law. Are those who practise certain kinds of conduct to be punished by imprisonment or fine? Administrative law, too, is involved. Must government introduce control mechanisms for the day-by-day supervision of some forms of interference, and is a system of licensing needed? And supposing that we concede that the law has some function, has it to be married in some areas with extra-legal institutional self-discipline?

What are these ways in which privacy is threatened? We have been familiar for a long time with officials asserting the authority to enter our homes and search them. Over two hundred years ago the courts established that fundamental principle of the common law that nobody, whether official of state or not, is *empowered* to enter our property. If he does, he must justify his trespass, and this he can do only by pointing to some law which specifically authorizes him. Here, then, we need watch only our parliaments. Unless they enact statutes which give oppressive powers to enter our homes, the courts can be relied on to protect us against trespasses by officials; they are subject to the same common law as the rest of us. That is why this aspect of privacy has been less controversial.

We turn next to the press and the mass media of communication generally. On the one hand there is great technical progress in obtaining and spreading verbal and pictorial information. Once

accustomed to this, the public then demand (or are encouraged to do so) more intimate and detailed accounts of the private lives of of those who, whether willingly or not, have become notorious.

The law of libel is not fashioned to handle this situation. It operates only where untrue statements are made which reflect on the character and reputation of another. Years after the event, an English newspaper seeks to increase its circulation by repeating in full detail the doings of Profumo and Christine Keeler as set out in the Denning Report commissioned by the government. The local press is backing a candidate in an election; it discovers that twenty years ago the rival candidate was convicted of stealing, and writes about this at length. No action for libel lies in this.

The urge for increased circulation in face of stiff competition and the public demand for the immediate inside story force the press to be importunate in news gathering. Mrs. Jones's baby has been killed in an accident. Why not arouse her in the middle of the night by crying "Police" and then photograph her, grief stricken, as she opens the door in her dressing gown? Or else harass her by continually telephoning her until she gives you a story? And then go to the hospital mortuary and photograph the battered corpse?

And of course the opportunities for television are greater. Film a local dignitary in the queue outside the bookshop in another city on the first day after the courts have removed the obscenity ban on *Lady Chatterley's Lover*. The powerful telephoto lens makes matters easier. A pop singer has moved into a house with his new girl friend. Hire a house in the vicinity and keep the camera trained on the bedroom to get shots of them making love. What difference does it make if the motive is more obviously social? Film Mrs. Smith at her front door turning away applicants for apartments because they are coloured. See how much alcohol the unsuspecting Mr. Green consumes at the bar; follow him out later to his car and encourage him in his inebriated state to say how many whiskies he has had and how far he is now going to drive, whereupon the bank of which he is manager fires him next day after he has been identified by them on the television programme.

For many years now, interception of communications has been common: it has always been possible to open another's letters. But tapping telephone calls is much more serious, and of course can now be done easily without the subscriber's knowing. It may be done by the intelligence service in defence of national security, the police in crime detection, the private detective in search of evidence for divorce. Legal remedies have been inadequate. Actions for compensation have not lain, and when the warrant of senior

government officials has been legally required there has been no check on whether that law has been heeded. English courts have always admitted evidence, even if illegally obtained. There has been no effective sanction against the interception, and it has spread.

More sinister has been the subsequent development of electronic surveillance devices, all to enable listening in. The simplest version calls for a microphone and transmitter no bigger than a sugar cube to bug the room. Alternatively, pretend to be the telephone engineer, fit a microphone to the handset, call the number any time and listen to the conversation in the room for an indefinite period, unknown to the subscriber. Or use a parabolic microphone, which will pick up every word spoken by those at whom it points, even a whisper half a mile away, and now even through closed windows by the use of invisible laser beams.

These electronic devices, freely purchasable, are used widely in business, and not merely in government service. They assist aggressive salesmanship. This is something more than the refusal to quit the front doorstep. The real estate man takes husband and wife to view the house, leaves them in a room at his office to talk over the matter in private, and having previously bugged the room, finds out how much they are prepared to offer. The firm which wants to learn about its rival's plans and know-how used to have to be content with bribing the janitor to hand over the contents of the boardroom waste-paper-basket. It now finds it much more satisfactory to bug the boardroom. Industrial espionage is a massive industry. Not all the methods are electronic. It is often better to plant a spy in the rival firm or to bribe an existing employee. The aim is sometimes to harm a competitor directly, for example by prematurely leaking the fact that the rival car manufacturer is putting a new model on the market shortly. Again the law's existing protection is thin — the law of theft does not meet the need.

The newspaper which wishes to expose the plans laid at a private meeting of the dealers' ring in the hotel before the auction to avoid competitive bidding, can do so safely; the dealers do not have "possession" of their hotel room, so that they cannot sue in trespass. Similarly immune is the divorce inquiry agent who bugs the hotel bedroom or who fires an arrow with microphone into the outer wall of an apartment — that outer wall will be in the landlord's possession, not the apartment tenant's.

The next threat to privacy we must consider is the computer, that "very fast and accurate idiot"; a threat because it can work out calculations so quickly and store so much information in a tiny space. Airline bookings are computerized; one can check a man's

journeys and the names of his travelling companions. Next, perhaps, will be central computerization of all hotel reservations; very significant for our private detective is the information that Mr. Brown and Mrs. Stone occupied adjoining bedrooms in seventeen different hotels last year.

Particularly important is the development of data banks. Information about all of us is collected within various manilla files: our tax returns, our health records, our employment records, our social security data, our bank accounts, our school and university records and our criminal records. Now information can be stored by computers and the state is taking the lead in doing so. In Britain this process is under way with the Post Office, taxes, vehicle and driver licensing, social security, medical records and (very important) police records including fingerprint collections. Of course a good case can be made out for all of this on grounds of efficiency. How long will it be before we proceed to the next stage, the interconnection of these presently separate storage systems? Then all the information in any data bank on any individual will be available in one print-out merely by pressing the appropriate button.

My emphasis so far with respect to data storage has been in the governmental arena. But we must not forget credit data. In all our countries, corporations are occupied exclusively with obtaining and selling information about the credit-worthiness of individuals: not only their incomes, debts, payment records, their bank accounts, but their drinking and sex habits too. And they have this data about most of us. Soon all this information will be computerized, and so will be immediately available on request. This will become the more important if, as seems likely, our countries use cash and cheques less and less. Our credit cards will more or less round off the complete picture of us, with our tastes, spending habits, interests and whereabouts duly fed into the centralized computer. And would it ever happen that the governmental and commercial data be married, perhaps through the identifying link of the social security number?

The law at present has little to say about these data banks. Why should it? But is the information necessarily accurate? I have not paid for my new television set because it was delivered in a defective state and the dealer has refused to put it right. Maybe because of this I am recorded as a debtor, a bad payer. And I shall know nothing about it and be puzzled by the subsequent refusal of other traders to give me credit. Further, I have no control over the use to which this information is put. Should I know what is recorded about me, and who has been told ? The common law normally denies a

remedy on proof of consent. A patient cannot sue the surgeon for amputating his gangrenous leg. Does every applicant for credit accept that the finance company will have access to comprehensive data on his credit-worthiness? Clearly if consent were to continue as a defence in this area its effects would be unconscionably wide.

One can raise these questions without demanding that the law prohibit centralized data banks. We know that technological progress cannot be resisted. There is obviously a case, on national planning grounds, for accumulating data centrally about individuals, as well as statistical information. We cannot uncompromisingly oppose arrangements which greatly facilitate the detection of criminals. Merely because technological inventions have speeded up the task of getting information which could have been acquired, however laboriously, before, we cannot outlaw them. The computer industry has done little to safeguard the citizen against abuses. Understandably, the industry looks to the lawmakers for direction.

On this side of the Atlantic you make very much more use than we, in England, have so far done of the polygraph or lie detector. I leave it to you to say whether I am praising you or criticizing you. In any event it is merely one aspect of a trend towards applied psychology in employment relationships. The prospective employee, or the staff member hoping for promotion or fearing dismissal, may be required to submit himself to interview by an industrial psychologist. Should he have to disclose his sex life, his attitude to sex, his political opinions, his religion? It is an open question when, if at all, there is an implied term in a contract of employment that an employee must submit to the polygraph or the psychologist. At least the law does nothing actively to discourage these intrusions.

I have been trying to indicate the ways in which privacy is threatened. Let me now make clear what the common law does to combat it. A victim of harm, however caused, who seeks compensation must have recourse to the law of torts. The common law of torts has in the past eschewed general principles. There have been no sweeping propositions, for instance, about intentionally or negligently inflicted harm. What we have had is a long list of separate torts, often overlapping, each with its own rules, within the confines of at least one of which the plaintiff must bring his case in order to succeed.

The most relevant of these torts is perhaps trespass, both to land and goods. This enables the occupier to sue someone who enters his land or searches his goods without the authority of law and without the occupier's permission. The occupier can be compensated for the damage inflicted on him, and might get an injunction restraining any further unlawful entry. By a recent decision of the House of Lords the damages are restricted to harm suffered — that award could include aggravated damages for injured feelings — whereas other parts of the Commonwealth have understandably refused to follow the House of Lords and can still award exemplary damages which go beyond compensation and seek to punish the defendant or to make an example of him. An action of trespass is restricted to those in possession. A hotel guest does not possess his room; nor does a hospital patient. The householder cannot sue in trespass to goods when his telephone is tapped; the telephone utility, not the householder, possesses the wires. If the cameraman spies on a household from the roadway, the occupier could sue because he is presumed ordinarily to possess that half of the roadway adjoining his building, but his wife could not sue if the house were not also in her name. These are serious limitations on the availability of trespass in the context of privacy.

The tort of nuisance is available if the occupier is harassed by interminable telephone calls. The man who constructs a system of mirrors in his garden to see what happens on the doctor's couch in his consulting room next door may also be suable. Again the reporter who pesters the bereaved mother is immune if the mother does not possess the house either solely or at least jointly with her husband.

When a man's privacy is intruded upon, he is often also defamed. But defamation doesn't protect the dead, so that Lord Moran in his memoirs and Hochhuth in his play *The Soldiers* could attack Churchill's character with impunity. In most jurisdictions truth is a defence; this leaves newspapers free to drag up the forgotten past, the more so as in England proof, in a libel action, of a conviction is conclusive proof of guilt. If a trader broadcasts the fact that *X* hasn't paid his bill or if the credit data record shows him to be a bad payer, he isn't libelled if it is true. And even if it is untrue, an agency might have the defence of qualified privilege when they convey this information, however false, in good faith to their clients. In a minority of jurisdictions — some Australian states for example — truth is a defence only if the defendant further proves that it was in the public interest to publish.

When a practical joker falsely told a woman that her husband had been injured, whereupon she suffered nervous shock resulting in physical illness this was held to be tortious. At first sight this seems relevant when the press importune the public. But so far the courts have refused to compensate for intentionally inflicted

emotional distress merely — they insist on proof of illness, and this will be hard to prove in most cases of this class.

We have seen that employees can sue employers for breach of contract, even on implied terms in a contract. It is unlikely that any of the techniques of industrial psychologists and even perhaps the disclosure of polygraphic records to third parties amount to violations of implied contractual terms. The employer could of course sue his employee who passed on trade secrets to outsiders.

Occasionally English courts of equity have issued injunctions to prevent breaches of confidence. The persons protected have been so exalted that one cannot be sure how broadly-based these decisions are. It is one thing for a judge to innovate in order to prevent someone offending Queen Victoria by copying her consort Prince Albert's etchings, or to prevent the Duchess of Argyll's sex life in the marriage bed from being serially narrated in the Sunday press by her ex-husband. How general will the courts declare this principle to be when the lower orders seek to rely on it?

English criminal law has little impact on privacy. Its effect is limited to the sporadic effects of a few random statutes, none of which had privacy in view. Thus it is an offence to intercept mail, but not to tap telephones. Certain officials, such as tax officers, may be punished for breach of confidence. Eavesdropping, at least of the Peeping Tom variety, could lead to a binding over to keep the peace under an Act of 1361. No offence is committed by selling or possessing bugging devices.

The law could discourage intrusion, especially by law enforcement officers, if it were to provide that evidence obtained by unlawful entry and search, by unauthorized bugging or wire tapping, was inadmissible in court. English law has taken exactly the opposite view. It regards it as irrelevant how criminal the methods were by which the evidence was acquired, as long as its cogency is unimpaired.

Granted that various ways of invading privacy are uncontrolled by law, is that something to complain about? Some argue that we cannot stand in the way of technological progress. We must learn to live with new inventions, to adjust our lives to fit in with them. Of course we must not turn our backs on fresh discoveries, but that does not mean we are their slaves. We welcome the automobile, yet we insist that the law be developed to make it as safe as possible; we control by law the noise it makes and the fumes it emits. And we know that without the law's help, there would be fewer safety features in automobiles. In the same way the law controls nuclear energy, welcome though this new source of power is. Therefore, although electronic surveillance devices, television, computers

and long range cameras are fine inventions, we are not precluded from invoking the law so that we get the maximum benefit and the least detriment from their application.

Nor will we concede to the state the right to act as it likes. It is true that when the courts first fashioned laws which protected the citizen against arbitrary conduct, the state was not the omnipotent do-gooder we know today. Yet in this respect we still look to the law to protect us; the state is not above the law. The state must still justify every interference with a citizen by pointing to a specific legal authority for what it does; the principle is the same whether the intrusion is by digging with a spade or through the sophisticated electronic devices of today's spy.

Another objection to law regulating privacy is that it is not the function of the law to pamper us, to encourage shamming, to pander to our neuroses. The law looks to matters of substance, not trivialities — that is why, for instance, we discourage breach of promise actions for heart balm. We protect against physical harm to the person or to property, we compensate for economic loss wrongfully occasioned. But why for privacy?

Dicey showed fifty-odd years ago that law and public opinion interact. And people do prize their solitude; they do demand limits on intrusions into their private lives, their families and their homes. They insist on their right to determine to some extent how much others should know about how they lead their lives. They feel that at present these claims are not realized, and that they are suffering unwarrantable interference. It may be retorted that people do not wish to be injured on the roads, and the law agrees; yet they still get hurt. So, it does not prove the need for law reform when unwanted events happen. There is a difference. Road users are hurt by careless drivers, almost never by deliberate running down. Those who intrude on our private lives do so intentionally, and normally to make money out of it. They will do it more and more if they are not stopped. There would be no need for the law to step up its role if the present rules, backed by the forbearance of government, business and the communications media, kept interference within bounds. They do not. Self-controlling institutional arrangements are not enough. We saw that recently in England. Public opinion condemned the *News of the World* for rehashing the Christine Keeler memoirs; the Press Council, an organization set up by the press but not recognized by Act of Parliament, roundly condemned its action, whereupon the *News of the World* continued with the series exactly as planned, and suffered no penalty.

The gap between what public opinion demands and what happens remains unclosed. How could there be a change without the

law's intervention? The force of public opinion can be effectively expressed only through powerful pressure groups. Business, the press and broadcasting, and government itself, have a vested interest in matters as they stand. There is no scope there, so that we are driven to look to the law for the necessary protection.

I propose to tackle first and separately computer data banks, for I believe that they need a legal system of their own. The characteristic of a sophisticated legal order is to prevent harm from occurring, and not to be content to redress the balance afterwards. Accordingly, it is not enough to enable investors duped by a false prospectus to claim damages (if they can get them) from the fraudulent promoters; far better to see that it does not happen by scrutinizing the prospectus before public advertisement. That holds good for data banks. Once the confidential and false damaging material has been released it will be too late to protect the victim, even supposing, for example, that he could prove that he had been denied promotion in his employment because of a print-out.

The answer is to set up by statute an independent commission to supervise these computer systems, including creditor reporting services, both those maintained by governmental institutions and by private enterprise. The commission should include scientists and technologists, expert in the subject, and lawyers. The statute would lay down in broad terms the commission's functions and delegate to it substantial rule-making powers both to meet the variety of special circumstances with respect to the different systems and to enable changes to be made in the light of experience and developments in techniques. Nobody, public or private, would be authorized to operate a data bank without a licence granted by the commission. In the case of private applicants, the commission would have to be satisfied of their integrity and financial stability. Licences would be issued always subject to conditions contained either in the Act, the commission's rules, or specified in this particular grant. All systems would have to conform to regulations which ensured security, the stringency of which would depend on the sensitivity of the data. For instance, where it was essential to prevent eavesdropping or radiations from the equipment, shielding materials such as metallic paper, copper screening, or circuit suppressors, could be prescribed, and the design layout would have to be approved by the commission before issuance of a licence. Sometimes scrambling or encoding of data would be required to prevent effective wiretapping. In complex data systems, hierarchies of data according to sensitivity could be formulated. All this would have to be built into the approved system. On all these matters applicants would be entitled to hearings if amicable agreement on conditions could not be negotiated. The licence would restrict the kinds of information to be fed into the licensed bank.

The commission would make rules about the use of the machines. The procedure would be closely controlled, so that, for example, staff operators would have to keep a log of all requests for data complied with. There is a case for controlling the staff themselves. In so fluid, new and expanding an industry, self-regulation within the profession would not be adequate. The commission would prescribe standards of character and competence, attainment of which would be a condition precedent to licence to operate. The commission would maintain an inspectorate to supervise compliance with its requirements, with powers of access to premises, data and documents.

The commission would be concerned that high standards of accuracy were maintained in compiling and collecting data, the more so with very sensitive information, and rules would be framed and enforced accordingly. Time limits for storage of various types of data would be prescribed and the appropriate destruction of old data required. For example, there must be a time limit beyond which a conviction for crime should cease to be recorded by a credit agency. The rules must give the individual who is the subject of the recorded information the opportunity to check the accuracy of that information. Certainly, every person, when first programmed, must be given a full print-out. The commission would resolve any disputes about the accuracy of a print-out and be empowered to expunge or amend. It may be too costly to entitle him to a free print-out of every subsequent item about him, but at the very least he must be entitled to it on demand and upon payment, and perhaps anyhow at prescribed intervals. The statute must also acknowledge his right to know to whom a print-out has been given, and for what purposes. Nobody outside the categories of person to whom the commission had authorized prints to be supplied should be supplied with information. This is merely a refined instance of the general need to have detailed rules within the public service, regulating the use to which information about individuals, whether in files or banks, can be put by government departments.

The commission would be empowered to revoke the licence of a data bank and of a member of its staff on breach of a condition in the licence. Criminal penalties could also be imposed for any breach.

Many of the points I have just been making are relevant to devices for electronic surveillance. In England the criminal law scarcely applies to them. In contrast, Germany, Norway and other

European countries have imposed criminal sanctions, and a representative conference of jurists, known as the Nordic Conference of Jurists, in 1967 proposed widespread controls. I believe that the use of these devices is growing so quickly, and the gains to the user are so great that restraints within criminal law are called for: liability to compensate for loss inflicted, when established, is not enough. Wiretapping should be prohibited. The exceptional circumstances in which tapping by a public officer in the interests of national security is to be allowed should be severely controlled. I am not content with the United Kingdom expedient of allowing a minister uncontrolled discretion to permit interceptions. I would prefer it to be in the hands of a senior judge, and permission to be for a limited period, with the annual publication of the number of taps authorized. Even tapping by a subscriber without the knowledge of the other party to the line should be covered. Bugging and other devices for electronic surveillance should be similarly prohibited. Breach of any of these requirements should be punishable by imprisonment or fine. The Nordic Conference would go further by licensing the manufacture, export, import, sale and use of these devices. On principle I support their proposal, but I doubt whether it can be fully implemented. Where the devices have no primary use beyond surveillance, licensing regulation, including that of devices already made, is feasible. The question is more difficult where they are capable of innocent use.

The stakes are so high in industrial espionage too that civil remedies are not enough. The English law of theft has at best marginal application. I would impose on those who acquire, and on those who take the benefit of, confidential information, criminal sanctions so harsh that the game would not be worth the candle.

A more difficult question is whether evidence obtained by criminal conduct in the form of tapping or electronic surveillance should be admissible in trial proceedings. I accept the American argument that this is the most effective deterrent against law enforcement officers. Yet the incidence of undetected crime is so high in England and the reliability of this evidence is so untainted by its mode of acquisition that I hesitate to advocate the American view that such evidence should not be admitted at a subsequent trial. After all, under my proposals, the law enforcement officer will have to stand his own criminal trial for illegally obtaining evidence, and stringent judicial application of that should be an effective deterrent. I have regarded the American rule as a confession of their inability to impose proper standards of behaviour on their police.

The outstanding question is how and when to compensate those

who suffer harm. Let me remind you of what has happened in the United States. Two distinguished jurists, Warren and Brandeis, published an article in the *Harvard Law Review* in 1890. They examined the scattered English decisions and from them deduced a general recognition of the legal right to privacy. Some American courts applied this reasoning. The American restatement developed it, encouraged by another jurist, Prosser, so that now most jurisdictions have built up, with only slight help from the legislature, general tortious principles of privacy. That summary shows dramatically how different American jurisprudence is from my own country's. Our courts never follow academic writings in that way. They have not developed any general principles about privacy. They would only move from case to case. Royalty and dukes can spend the money on speculative litigation, but the rest are more timorous. It would take another hundred years for our courts, unassisted, to reach the present American position. That pre-supposes that they would be willing; in fact, when issues of policy are involved, they say openly that it is Parliament's job to decide. Further, the American approach has not proved sufficiently flexible to cope with the important new problems: telephone tapping, electronic surveillance, polygraphing, and computerization have all escaped from the American judge-made net. Indeed the American law of privacy has had little impact. For all these reasons, our solution must lie in creating a new tort of privacy by Act of Parliament. In framing this we can profit from American mistakes and inadequacies.

Undoubtedly this is the most difficult task of all. I have never seen a wholly satisfactory privacy Act. Even British Columbia's commendable Privacy Act, 1968, does not meet some of the points I now propose to make. I do not have a draft statute to read out to you — not that you would wish it. I shall merely draw guide lines. But however good a compensation Privacy Act is, it must not stand alone. The other legal devices I have been talking about must be made to mesh with provisions for compensation. Privacy for this purpose is the right to be left alone. The invasions from which protection is needed are mainly two: offensive intrusions and unreasonable publicity. Publicity must cover also communicating information to third parties even though it is not communicated to the public generally. For example, the operator of a data bank must not be allowed to pass on harmful information even to one of his customers; it is not sufficient to deal with the case where a list of the plaintiff's past debts is exhibited in the office window fronting on to the highway. In our law of defamation there is a statutory defence where the defendant proves that he did not know

that his statement was defamatory of the plaintiff and could not by taking reasonable care have discovered that. Privacy should be handled in the same way; the innocent invader should have a defence.

The major area of difficulty with legislation is the press and broadcasting. Here one has to consider a particular country's constitution and its attitude to the press. Englishmen would find freedom of the press unacceptable to the extent to which the United States has it. Trial by newspaper, however prejudicial to the accused, is commonplace there. We reject that. We say that a prisoner must have a fair trial, and that newspaper editors who defeat the course of justice by publishing beforehand their own views on his guilt must go to prison for contempt of court. Similarly we should not follow the United States Supreme Court when they recently held that the press was not liable for a negligent invasion of privacy; we would say that the press has the same duty to take reasonable care as anyone else. Above all, I trust that we should not take the easy way out and say that the difficulties of framing a privacy law for the press are so great that they must be excepted from its application altogether. Nor should we be deterred because editorials will unanimously condemn any proposals to curb press freedom.

There is a tendency in United States decisions to confine privacy law to true statements and leave the falsehoods to defamation. Yet privacy is menaced by the untrue often in cases where an action of defamation is not, at present, available: libelling the dead to the pain of near relatives is a clear illustration.

Most sponsors of a code include a general defence of public interest. They feel that such a clause is essential if press opposition is to be overcome. There are dangers in this. Take the United States. The courts will say that it is in the public interest to publish anything newsworthy; many United States courts seem almost to be holding that an item is newsworthy if the press says so. I cannot support such a wide defence of public interest. Nor am I sure how competently English judges would assess public interest in this policy-making area. The more specific the Act the better. It will be fairly easy to define the instances where statute authorizes physical intrusion and the conditions to be satisfied with regard, for example, to national security and crime detection. The Act must not allow government to do as it pleases under the guise of public interest. Even with regard to press publicity, much can be done. Some European states prescribe the number of years after which raking up the past is forbidden. Lawyers there tell me that this law works well.

I have similar hesitations about incorporating the defence of privilege, which is familiar and far-reaching in defamation. For example, whatever the law of privilege in libel might be, when a credit agency supplies a print-out to a customer the common interest of the parties could not be accepted as a privileged occasion in an action for infringing privacy.

Even the traditional defence of consent would have to be looked at circumspectly, because so often here parties are subject to psychological pressures or give their alleged consent while under emotional stress. A narrow definition of voluntary consent would be needed, a stricter definition than our courts have often applied in other areas of tort where consent is relevant.

Various remedies should be available to the victim. By injunction he should be able to restrain repetition of the offensive behaviour. If the wrongdoer has profited let him be required to account to the victim for that gain; this will be especially important for industrial espionage. The victim should also be compensated for any loss which he has suffered.

Privacy, then, is an area where the conflicting tugs of freedom and responsibility must be adjusted. We cannot expect the press, or business generally, always to behave responsibly without the law's prodding. We must beware of doing harm under the banner of freedom, whether it be freedom of the press or freedom of the individual.

We all realize how important it is to preserve our liberties. I know that Canadians are as jealous of their freedoms as any other nation: the Dunning Trust lecture series is further witness to that. We see, too, that a liberty once lost is not easily regained. We are menaced in all directions, and the threat grows daily. There is no excuse for inertia. We know exactly what interferences tomorrow will bring. Peace of mind is treasured by all of us. We need the help of the technologist, the scientist, the politician. The law, too, must help both in creating an appropriate framework and in moulding public opinion. The sooner we act to protect our privacy as far as is just, in view of the competing demands of free communication, of government and business enterprise, the better. There is no time to lose.