THE RIGHT TO KNOW vs. THE RIGHT TO TELL

Daniel J. Henry*

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. ... That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them ... like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.
>
> Thomas Jefferson

The same can be said about information. Experience has taught me that information, like water, floats to its own level. As long as we live in a community and let information out about ourselves at some point in time, that information will find its natural audience. Our obsession with controlling information about ourselves is largely futile and often counterproductive. That has been proven a number of times in Canada in the past. It will be proven again.

For example, the Defence Department tried valiantly, but vainly, to suppress information about its activities at the time of the Somalia controversy. It went so far as to change the name of a class of documents being sought by a CBC journalist so that it would not have to admit that it was continuing to produce them. The journalist found out about the name change, and in the process caught the Chief of Defence staff lying about their existence.

A second example became clear when natives barricaded themselves at Gustafson Lake, B.C. Bans on the interception and use of radio-based telephone conversations did not stop anyone in the town from knowing what the police and the natives were saying to each other during their negotiations.

Counter productive uses of information can also arise. Mr. Friedland, a successful stock promoter, was convicted of a drug offence early in his life and was subsequently pardoned for it. When CBC's program *the fifth estate* did a story about a gold mine he was involved with, they found out about his conviction and pardon. He was afraid that they would use that information in their story – which, incidentally, they had no plans to do. He sought a sweeping injunction against CBC even mentioning the injunction, let alone broadcasting the information. He took the position that his pardon wiped out his conviction for all time and for all purposes, forgetting that references to it were

---

*Mr. Henry holds the position of Senior Legal Counsel at the Canadian Broadcasting Company in Toronto. The presentation which this paper is based upon was given at the Human Rights and Technology Conference, held in Fredericton, New Brunswick on 28 April 1997. The views expressed in this paper are those of the author alone and not necessarily those of his employer.

contained in old clippings in newspaper archives and libraries. It was part of history. Mr. Friedland never received his injunction and brought more attention to the pardon that he was trying to suppress than *the fifth estate* would ever have given it.

In any discussion of the right to know, we have to begin with the realization that we do not control information about ourselves, and we probably never will. The most we will be able to achieve is control over some information, in some hands, at some times. In determining the ideal level of control, we should not ignore the costs of achieving it. This does not simply refer to the financial costs, which can be substantial. Regulation of the way we work, record events, and ultimately think exacts a significant human cost as well.

The Quebec law protecting personal information in the private sector is the only legislation in North America that regulates how enterprises in the private sector deal with personal information. It is no accident that it has the following caveat built into its very first section:

> This Act does not apply to journalistic material collected, held, used or communicated for the purpose of informing the public.[1]

Journalists would not be able to function if every word they wrote about someone had to be classed as personal information and made subject to the Act's restrictions on collection, security, and review. But journalists are not the only ones who need this freedom. We all do.

Technological developments may assist us in fitting within this kind of journalistic exemption. Today, every enterprise with a home page on the Internet informs the public, and also collects information for the same purpose. In some ways, we are all becoming publishers.

In Europe, the European Union's Data Protection Directive is about to cause even traditional "journalists" trouble. It places all digital information on someone under the same regime. Now that the radio and television industries are converting their equipment and facilities to digital formats, their journalists will be caught as "processors of digital information relating to individuals" and will have to open their "personal files", pre- or post publication, to the individuals concerned for their scrutiny. There are concerns that when the directive comes into force in 1998, doorstep interviews with reluctant subjects and hidden camera images of fraud artists will not be usable.

The argument for greater freedom in record creation is not an argument for freeing public servants of the need to be subject to access to information or related privacy legislation. It is an argument for a less mechanistic and mindless application of

---

[1] *An Act respecting the protection of personal information in the private sector*, S.Q. 1993, c.17.

protection for every scrap of information that happens to have a personal identifier. It is also an argument for being wary about extending the access to information and privacy straightjacket to everyone in all sectors of society in order to achieve what are realistically limited objectives at a time when the harms have yet to be really proven.

I have followed, with interest, the public debate on where to draw the line between private and public information. For almost 20 years as a lawyer at CBC, I have advised journalists on what they can publish safely. In and around that time, "privacy" has developed its cachet, and there has been a tremendous expansion of laws and institutions and the development of a cottage industry addressing and protecting it. A freedom of information act could not be passed in any jurisdiction, for example, without passing corresponding legislative provisions. These would not only protect privacy, but also nullify many of the benefits of the freedom of information legislation itself, not to mention provide new restrictions on public access to a great deal of what was once easily accessible information.

As a lawyer advising journalists, I learned early to resist the temptation while reviewing a potential story to recite to them all the ways that information cannot be published or broadcast. I am continually surprised by the creative approaches they come up with to enable them to tell their stories on the air without legal restriction in the exercise of their freedom of expression.

Provincial privacy statutes exist in five Canadian provinces to protect people from surveillance, the theft of our personal papers, and the exploitation of our rights of publicity. The Criminal Code appears to protect us from illegal wiretapping, interception of cell phone conversations, and personal surveillance and harassment.[2] The common law protects us from misuse of confidential information. While these laws may affect, in some small measure, how information comes out, they have had practically no effect on the media's ability to collect the personal information and publish the stories they deem to be of public interest.

Legislative efforts designed to restrict information flow are generally unfocussed, misleading as to their effectiveness, paternalistic, and lead to distortions in information flow that benefit those with power, at the expense of a better functioning democracy. Legislative favour of late has rarely been bestowed on those supporting greater information flow. That alone should cause concern for a response in favour of accepting their call to do something more about keeping records private. In addition, those efforts seem to ignore freedom of expression. This freedom is recognized internationally in the UN Declaration of Human Rights, which states:

---

[2]R.S.C. 1985, c. C-46. See ss. 184, 264(2)(c), and 423(1)(f) and (2).

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[3]

Important to this freedom is the need to be able to think, write, and gather information relevant to that creative process without government interference. That means being able to keep notes that record random thoughts about real people and conversations with them, exploring potential responses to real events, and keeping those records without feeling the need to justify having done so. Laws which seek to identify, order, and supervise virtually any record containing personal information, whether or not they are released, relied upon, or sensitive, are destined to make criminals of us all, promote disrespect for law, and are doomed to failure. Demanding the right to monitor any and all the information kept by others may protect the privacy interests of the person making the demand, but it is a gross intrusion on the rights of others, as record makers, to be left alone and to express themselves freely. We know from our experience with the public sector that such laws discourage record taking, encourage the creation of phony records suitable for public viewing, and ensure that real information is kept under wraps and is used secretly by those with preferred access and power.

The marketplace is not perfect, but it is a great leveler. Ask the Chinese government how they feel about public access to information in light of their experience with the democracy movement and their attempt to control their peoples' access to the Internet. When people get access to information wonderful things can happen. For example, my wife made contact recently with a friend she had been trying to find for years. She found her through an Internet people search. Their friendship has flowered since. Privacy regimes restricting access to this kind of information could have been justified, but we are living proof of the delight that can happen because they were not.

As a general proposition, personal information should be widely available to all, with each of us having access to a means of contributing to its clarification. Freedom of expression, as a constitutional right, should be presumed and any exceptions based on privacy should be limited and extremely well justified, even though wide access comes with a price. Governments can more easily weed out the people or peoples they deem to be problematic and criminals can find targets more easily. However, these are remote possibilities, and each of us should learn survival skills in that event. There will always be steps you can take to protect yourself.

I am not an opponent of privacy, but a proponent of it, yet on a realistic basis. The police should not use photo surveillance of our highways to impose a rigid sameness on every driver, in every situation, for the sake of their convenience. However, they

---

[3]Article 19.

should be allowed to use the information to gather statistical data, to give traffic and weather advisories, and to catch the dangerous drivers that would otherwise elude them. The information should only be used for acceptable ends, and the subject of that information should have the right to address misuse of it whenever and wherever it is discovered.

Experience suggests that privacy laws are enacted because of fears based on very little real evidence of harm. Ontario reduced public access to car ownership information based on only a few cases of abuse. Information that was widely used before the restrictions, with few difficulties, is now more difficult for everyone to get. A government bent on solving everyone's problems now denies everyone that use, on the basis that it knows best.

If personal information remains widely available, and if it is correct to assume that information finds its natural audience, Canadians generally will ignore the series of personal but historical records that each creates in the course of our lives. In the information deluge, we as individuals will continue to be insignificant to them. Our homes are in the open now and we can be found. The reality is that we are not sought out. The thieves we worry about seem to be busy elsewhere.

My wife's Aunt Nettie lived in New Jersey. She hardly ventured out for fear that there was someone lurking behind every bush waiting to mug her. According to my wife, the world was a much safer place when Aunt Nettie was alive. Now that she is dead, she has freed up a lot of muggers. Incidentally, Nettie lived her entire life in peace, as do most of us concerned about these issues. Obviously criminal acts do occur. The point, however, is that we cannot let the criminals win by refusing to live our lives confidently and freely because of statistically insignificant fears. We should take precautions that do not make us nuts, but we should not rearrange our lives completely to try to control potential, but remote, threats.

Who cares if my property ownership is on the Internet? Who cares if some other financial instruments disclose the money I own or owe, and that is available to those who care to find it out? Who cares if information about my buying habits is outside my total control? (My buying habits are out of my control anyway!) I am not the sum of my statistics. My soul cannot be stolen by someone who has many of the details of my life. I am and will remain me, a human being, always in control of who I am. I can fight misinformation and misuse of information about me. I can also give up, change my name, convert my holdings to cash, buy a boat and live on the high seas. But for now I will live here in Canada, without being overcome by electronic information fear.

Tempting as privacy rules are, we should be wary of adopting them until there is proof of widespread abuse that cannot be alleviated by free market technological solutions. Those interested in privacy will always have specifically tailored technological options to help them.

Blanket legal solutions lead to strange results. In Yellowknife, CBC was prosecuted for publishing the name of a sexual assault complainant contrary to a court order banning generally that type of publication.[4] The statutory ban was designed to protect the privacy of someone making that kind of complaint. However, in CBC's case the complainant, whose identity CBC published, was dead at the time. Her death came while in the custody of the police, and a public coroners inquest was held into the whole affair. Everyone who knew her knew the circumstances of her death, but according to the Crown prosecutor, CBC was prohibited from identifying her in its reports anyway. CBC took the position that the ban did not apply after she died, and news reports would be significantly enhanced by the use of real information. But so far the ban knows best. CBC has been convicted in one case that will be appealed, and will face another trial on May 7 for a related story on the coroner's inquest.[5]

It is not wrong to want to know who your neighbour or business acquaintance is. Information is not simply fodder for idle gossip. It can be important to your well-being. It can save your child from abuse at the hands of someone you might not otherwise suspect. It can save you from doing a business deal with someone who has taken others for all they are worth. It can give you comfort in dealing with someone you have just met.

Before this recent fascination with privacy, Canadians developed a number of legal regimes with the exact opposite approach. We insisted that a variety of kinds of information be public, for public benefit and safety. The result was the development of public registers of property ownership, tax records, judgments, writs of seizure, bond issues, securities issues, bulk sales, car ownership, vital statistics, wills, marriages, election rolls, police arrest, occurrence reports, etc. All of this is replete with what we now call "personal information" that would be kept from being released today except for the fact that we developed a practice of doing so long ago. Yet, some of this information has been taken out of the public domain in some jurisdictions. Amazingly, some of this public information is only permitted to be public now for short periods of time and only on paper.

Metropolitan Toronto is one place where Occurrence Reports and Arrest Notices once routinely identified those involved in incidents which the police had investigated. The media would take that information daily, and speak independently to the people involved, occasionally interviewing them for their stories. In only a handful of cases,

---

[4]*R* v. *Canadian Broadcasting Corp.* [1996] N.W.T.J. No. 115 (Terr. Ct.) (QL).

[5]The CBC was subsequently acquitted on the second charge. See *R* v. *Canadian Broadcasting Corp.* [1996] N.W.T.J. No. 120 (Terr. Ct.) (QL). Both results were appealed together to the Northwest Territories Supreme Court. See *R* v. *Canadian Broadcasting Corp.* [1997] N.W.T.J. No. 83 (Terr. S.C.) (QL). There the appeal against the conviction was dismissed, while the appeal against the acquittal was sent back for a retrial. The CBC is currently appealing this decision. A third charge was imposed against the CBC for its report on the acquittal. This charge will be dealt with at the resolution of the prior charges.

people complained about the media's approach to them. Ontario's *Municipal Freedom of Information and Protection of Privacy Act* changed the rules.[6] Now, Occurrence Reports are issued by the police but without identifying information. The media still refers to them, but are now barred in practice from using them to make direct contact with those involved. This really does not have a practical effect. The media follow the police around. Neighbours call the media. Police communications are monitored. Cameras are everywhere. The important stories still get on the air, but with more difficulty. The less important stories do not get covered, however they would have received little coverage in the first place.

Arrest Notices are still provided to the media on paper daily with all the pertinent information, but a recent attempt by a Toronto newspaper to get computerized access to this information was denied by the Information and Privacy Commissioner's office. It held that despite the fact that this information was public record, it would be an unjustified invasion of privacy to permit easy access to it, rather than requiring someone interested in it to do a diligent search of court files, county archives, and local police stations throughout the country. The fact that the newspaper could create its own computerized records over time did not seem to be a factor.

In Quebec, by contrast, the SOQUIJ court data system has permitted anyone, anywhere, to get a complete province-wide civil and criminal court records on anyone by computer. Public records are only public if they are accessible. The Toronto decision acts as an incentive for criminals to relocate to that city, and puts the community at risk because of its inability to learn about their criminal records easily. Even though criminal records catch up to most everyone, the harm is in the delay.

Privacy regimes are misleading because they appear to protect privacy, but do not. They cannot. As long as anyone knows the details, the information will be passed along.

These days, for some kinds of information, the media may be the last to know. As audiovisual Internet communication becomes more and more the successor to the simple telephone conversation, people will show and tell everything they know anyway. At that point, databases will be everywhere, and no one will comply with any privacy laws that purport to apply.

The most notorious example in recent memory of an unsuccessful attempt to restrict information flow about a case that interested millions of Canadians was the publication ban on the trial of Karla Homolka.[7] The ban was not issued in the name of protection of privacy, but in the interests of Paul Bernardo's fair trial. For the sake of argument,

---

[6]R.S.O. 1990, c. M. 56.

[7]*R* v. *Bernardo* [1993] O.J. No. 2047 (Gen. Div.) (QL).

the purpose of the ban does not matter. Its effect does. There was already tremendous interest in the case in Southern Ontario because of the conscripting of the community to find those responsible for the abduction of Kristen French. The ban attracted the interest of reporters around the world. American newspapers began printing details that were smuggled across the border. American television stations began broadcasting stories over the border. Canadian cable companies tried valiantly to block out whole newscasts on American stations, but information slipped through. Rumours abounded until they took on all the indicia of fact, save for the fact that they were not true. The Internet sported newsgroups dedicated to defeating the ban. If this happened today, U.S. newspaper web pages accessible to all Canadians, would deliver the news directly to our homes in full colour on command. At least one member of the Ontario Court of Appeal panel hearing the media's appeal of the ban scoffed at arguments that suggested that the ban ought to be lifted since it was not working anyway. Commenting from the bench he said that lifting the ban would only reward lawlessness.

In a different case decided about the same time, the Supreme Court of Canada showed considerably more realism. In the course of removing the publication ban which interfered with the broadcast of CBC's movie *The Boys of St. Vincent*, the Court noted that:

> [R]ecent technological advances have brought with them considerable difficulties for those who seek to enforce bans. The efficacy of bans has been reduced by the growth of interprovincial and international television and radio broadcasts available through cable television, satellite dishes, and shortwave radios. It has also been reduced by the advent of information exchanges available through computer networks. In this global electronic age, meaningfully restricting the flow of information is becoming increasingly difficult.[8]

In an earlier case, the Supreme Court held that theft of confidential information was not a criminal offence. In the course of that ruling, the Court made this observation:

> It is understandable that one who possesses valuable information would want to protect it from unauthorized use and reproduction. In civil litigation, this protection can be afforded by the courts because they simply have to balance the interests of the parties involved. However, criminal law is designed to prevent wrongs against society as a whole. From a social point of view, whether confidential information should be protected requires a weighing of interests much broader than those of the parties involved. As opposed to the alleged owner of the information, society's best advantage may well be to favour the free flow of information and greater accessibility by all. Would society be willing to prosecute the person who discloses to the public a cure for cancer, although its discoverer wanted to keep it confidential?[9]

---

[8] *Dagenais* v. *Canadian Broadcasting Corp.* (1995) 120 D.L.R. (4th) 12 at 44.

[9] *R* v. *Stewart* (1988) 50 D.L.R. (4th) 1 at 11.

While the Supreme Court clearly understands that there are limits on a court's ability to order information to be suppressed, it has also spent considerable time defining the constitutional parameters of privacy in the context of protections against unreasonable search and seizure by the police. In the *Duarte* case, the Court sanctioned the difference between knowing and telling in an electronic context.[10] It would be allowable for an informer to tell the police and testify about his conversation with the accused, but the court refused to permit the police to use in evidence audio tapes of the same conversation made by them without the knowledge of the accused and without judicial authorization. Mr. Justice LaForest, writing on behalf of most of the court, said:

> I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.[11]

In this era, all information is the same. It is bits and bytes, deliverable in a variety of forms. In time, the courts will become more comfortable with this.

Soon the Supreme Court will hear an appeal from a case brought by Pascale-Claude Aubry against the arts magazine *Vice-Versa*. Ms. Aubry was sitting on a doorstep beside a sidewalk in public on St. Catherine St. in Montreal when a freelance photographer Gilbert Duclos walked by and snapped her picture without her knowledge. He gave it to the magazine for free. Three judges of the Quebec Court of Appeal held that publishing it without Aubry's consent was a violation of her right to anonymity. The majority allowed her award of $2000 against the magazine to stand.[12] The media are seeking to intervene in the case to point out that their archives are filled with images of people who have not specifically consented to being photographed and who cannot now be found for the purposes of obtaining consent. As well, taking and

---

[10] *R* v. *Duarte* (1990) 65 D.L.R. (4th) 240.

[11] *Ibid.* at 253.

[12] The Supreme Court upheld the award against the magazine in its decision 9 April 1998, affirming the result in the courts below: see *Aubry* c. *Editions Vice-Versa Inc.* [1996] A.Q. No. 2116 (Que. C.A.) (QL). The Supreme Court held that under Quebec law the right to privacy includes the right to control the publication of one's image, except in circumstances where the public interest is conclusive, taking into account the nature of the information and the situation of those concerned. The public interest would be conclusive when the person is part of a public activity or event of public interest, is a public figure, is incidental to the main subject of the photograph, or has given his or her explicit or implicit consent to publication. It is likely that the Court's decision will lead to further litigation to clarify the law in this area.

publishing pictures of people without their individual advance consents or vetoes, which is a better way of looking at it, has traditionally contributed to free expression. As publications like *Life* magazine demonstrate, this freedom has added enormously to our cultural heritage, capturing in single images ideas, situations, and moods. The question remains as to who Ms. Aubry would sue if she did not know the photographer and her picture found its way onto the Internet.

Regardless of how the legislation and the cases resolve these privacy issues, information will find its natural audience. The police can get information from their informer, and can obtain judicial authorization for a wiretap to record the audio evidence of the informer's conversation. This is exactly what the Supreme Court told them they could not otherwise use.

Privacy acts that prohibit surveillance, permit, according to their terms, publication of information in the public interest. Information that is suppressed by freedom of information and related privacy laws, is routinely available from secret sources.

Whatever we are afraid of, suppressing information is a losing battle. We should invest our energies in ensuring that whoever uses the information has accurate and up to date information, and that they use it appropriately when it has any real ability to affect us.

The Internet tremendously amplifies the need for people to be aware of limitations on their right to publish information they obtain. Canadian law is not the only concern. The recent case brought by Germany against the German manager of CompuServe for aiding in the distribution of child pornography demonstrates that. They maintain that he could have prevented the transmission of images of violent sex, sex with children, and sex with animals, not to mention pictures of Adolf Hitler and Nazi symbols like the swastika available around the world on the Internet. At this point, we are all left to assess the practical risks associated with a lawsuit or prosecution in a particular foreign country each time we publish material of interest there. An interesting question that will take time to resolve is whether putting material on a web page in one country and making it available for downloading elsewhere constitutes publication in that other country. Arguably, no publication takes place until the recipient voluntarily downloads the image, an action which the web page creator cannot stop.

Protection is afforded to each of us by laws other than invasion of privacy. In most provinces invasion of privacy has rarely been necessary to remedy civil wrongs. Laws exist to regulate defamation, negligent misstatement, false advertising, copyright and trademark infringement, unfair competition, breach of confidence, and more. Without developing laws of privacy further, the right to tell is not without constraint. The good news for access providers and publishers is that there is ample legal protection available to guarantee the right to tell as well.

While I obviously have doubts about the value of our collective focus on privacy, like many of us, I have had some concerns. I fell recently and scraped my knee just outside a lab in Scotland. Since the news came out about the cloned sheep, I have had nightmares of my DNA being scraped off the sidewalk, a duplicate being made of me, all the public information about me being absorbed by him, and being replaced by him at home and at work. I am not worried about that anymore. It is obviously a lot of baa...loney.

Send in the clones...