PRIVACY IN THE INFORMATION AGE... *DO YOU HAVE ANY?*

© VINCENT DI NORCIA 1990

> The hare of Technology races ahead. The tortoise of legal protection dawdles aimless, lost, bewildered, far behind.
>
> Michael Kirby, Australian High Court Judge

AN MP'S FOLLY

At a 1990 New Democratic Party convention three leadership contenders and a few others agreed to wear small lapel radio mikes, not bugs, to record conversations for a CBC-TV Journal program camera crew who followed them. This was for a documentary, because, as Mark Starowicz, the CBC-TV producer, claims, "they agreed to be open [and to] share our enthusiasm for showing the tensions and drama of a major convention ..with the public. Jim Fulton told everyone he talked to he was wired. But NDP MP Simon de Jong was having a `private' conversation with Dave Barrett. It was not bugged—or so he thought. He did not tell Barrett he was still wired for the CBC-TV interview. He had also forgot to shut off his mike; but it was prominently displayed on his tie. The result was, that discussions about a deal to support Barrett in return for becoming party whip were broadcase unedited and raw on the CBC Journal three days later.

Canadian Federal criminal law allows the taping of private conversations if one party consents, so nothing illegal transpired. But the ethics, and intelligence of de Jong's actions and the CBC news program, The Journal's are open to question. "We do not believe in bugging or.entrapment. We do not even believe in the right to report everything we lean in ..a story... There is always a tension between the right to privacy and the public's right to know" says Mark Starowicz, its director.

THE OLD GROUND RULES

But it is clear: I can bug you if we talk and it's legal. And it can be reported on the media. The media are shameless, and exposure seductive. Trust no one, certainly not the media. Their interest isn't yours, and it isn't necessarily the public's. It's mainly in getting interesting information for their audience. Never agree to an interview without setting out the ground rules on taping, quotes, etc, in advance. Also, we need to change the one person consent rule for legalized bugging. All must consent, or else it should be a crime.

MONITORING MADNESS: 3 CASES

In the US a large manufacturing company hid mikes in employees bathrooms to ferret drug sales/use. They were discovered and the union grieved. A bank did a random chenck of employee computers found personal letters and an income tax prep program on one person's machine; she was warned against using it for personal business. 2 workers who got into a fight as they left the factory were taped by the parking lot security video cameras and later fired. In all 3 incidents workers felt their personal privacy was invaded and they protested, successfully in the last case. In all there management's right to monitor work, the privacy of employees at work, and away from work is in question. Positive drug tests of employees -notoriously unreliable- sometimes show traces left from drug use over the weekends has led to firing workers.

Moreover Intensive hidden monitoring of the workers at work and elsewhere, is increasingly common, especially in many financial, telecommunication and computerized operations. Silent Surveillance is the other side of IT. Video cameras, recorders, Pagers, intercoms, phones and

computer terminals all allow omnipresent ongoing, hidden monitoring of their users. They facilitate monitoring of how much work is done, how fast, how well (error rates), when, time at / away from work, outside communications, etc. Typically the surveillance is silent. One program CNTRL managers can observe all input and output on employee's computers. This is logged for use in disciplinary and legal proceedings. Another program can pop the following message up: `You are not working as fast as the person next to you.' Bell monitors 76 measures of operator performance including Average number of seconds in dealing with customers, of keystrokes operator used, screenings to find a list, times, and note whenever these times fluctuate too much. Pacific Western Airlines which owns Canadians and Wardair used a similar system with its reservation clerks, but in order to get them to compete against each other: "Compare yourself to your friends. Compare yourself with those who aren't your friends. Are you pulling your weight in the office? When the monthly stats are published ensure you're not dragging down your team and your office." PWA periodically tapes employees conversations too. Air Canada measures reservations clerk productivity per hour...

Much of this is a legitimate part of performance supervision and communications, only now electronically enhanced. In a 1986 study, one of whose authors, Frank Safayeni is in our Management Sciences dept., Workers in 3 insurance companies and a financial institution complained about the , computerized performance monitoring and control system (CPMCs) because of its overemphasis on quantity of work as against quality of performance> The intensive monitoring caused. CPMCs certainly yielded increased accuracy about worker performance, higher productivity more managerial control; but this was counterbalanced by increased stress, decreased quality, less worker autonomy, and poorer customer service, less satisfaction and greater stress. The demand for speed led claims workers to adopt the attitude: when in doubt pay out. The system thus may have been costing the company higher claims too.

Workers were not opposed to the computerized monitoring in principle. Indeed some Bell operators can use the ratings to check their own performance. The Com. Workers of Amer. union negotiated a ground breaking contract with Equitable Life assurance Society, giving claims processors access to inf4 on the company's productivity system and the right to view their individuals records and check for errors. Pay is still linked to productivity, but employees can grieve if they think the computer has erred. CUPW succeeded in eliminating individual computer surveillance and video camera monitoring (unfortunately?). But no laws govern such computerized surveillance systems. "It is not the Technology itself but rather how it is used by management" that determined their reaction. If CMCS is a "big stick" or deskills work and worker autonomy, robotizes workers then it is merely a computerized enhancement of `scientific management'.

Electronic monitoring and house arrest is now being developed as a substitute for prison in many crimes. It has numerous advantages, if it is used to decrease incarceration, and is flexible enough not to make the house an even worse prison. At least the criminal knows he is being monitoried and in some cases can chose it instead of imprisonment. This reveals that the issues are not so much the Technologies as the values they represent and the organizational setting in which they are introduced and operate. I will term this the socio-technical ground rules of IT.

PROGRESS TOWARDS PANOPTICON:

If you can tell us electronically, we can watch you, same way. Or, any telephone or cellphone is a microphone; and info channels go in both directions. So who's telling whom what, when, and how?

The Boss as Big Brother: Technically Watching workers
Electronic bracelets and house arrest:

Shopping by Minitel or Alex & Equifax Monitoring your life and values and what else?

Instead we need progress, plain and clean: Informed consent at least, participation and redesign at best. Most IT systems are naturally bidirectional in design. It is simply a matter of `taking advantage' of the `two way' street. This can be done positively to enhance communications and participation or negatively to enhance control and surveillance.

FILE FETISHISTS

Big Brother is watching you, with the information you supply. and Big Brother is not always the state; He's often a business. In applying to American Express for a card for instance you are asked for your bank accounts. A Mr. Ray Parrish of NYC had his `privileges' suspended because AE checked his bank account balance and deemed it too small to pay his monthly charge. Welcome to the information age. You can't leave home without it. The financial services industry foundation is of course money, numbers; just what computers love to crunch, and what telecommunications enjoy moving around; taxes and census data aren't much different. And in order to get most services, private and public, you have to offer all kinds of personal and financial information: loans, bank accounts, phones, family members, work, etc..

If that information stayed with the company you gave it to things would be bad enough, as the AE story shows. But it doesn't. Personal and financial information is exchanged, amassed, massaged, matched, sold, and often corrupted and misconstrued by all kinds of other companies and agencies for all kinds of purposes distant from the original purpose for which it was collected; and totally without your knowledge or agreement. Electronic funds transferring systems move information about your banking, investing and purchasing all around the continent with ease. Worse, it's almost impossible for you to find out who has what information on you where and how it is being used. "For very little cost anybody can learn anything about anybody."

Even US Banks are using and selling confidential information about their clients. Canadian bank laws codes forbid such practices. The result is, in *Business Week's* words, "Almost no information isa private. Only rarely moreover can individuals find out that information on them is being used" and how. Governments collect and exchange masses of data abnout citizens, and build dossiers.

3 major US credit bureaus, to which most Canadians data goes -in itself a weakening of our economic autonomy-- TRW Equifax and Trans Union Credit Information have 400 million records on 160 million individuals. They believe in one kind of privacy: they guard their records against stealing; but they sell it `freely', They'll package it 300 different ways broken down into various social categories, from possible bankrupts, to individual credit reports. They in turn serve 300 smaller local credit and collection agencies. The bureaus get their data automatically each month banks and retailers, etc send them electronic files detailing purchasing and payment activities of early every consumer in n. America: includes mortgage, credit card, bank accounts, income, family, work histories, driving records, legal actions, SINs. This stuff is repackaged and sold by the bureaus.

Jeff Rothfeder a *Business Week* reporter, showed how permeable the system is. He simply called a dozen superbureaus and chose 3. He identified himself as "a McGraw Hill editor who might be hiring someone", using the names of 2 colleagues. He signed a legal form declaring himself a customer authorized to buy credit reports; it was accepted by fax -which isn't legally binding. Another bureau's ads offered services like instant nationwide tracing of social Security numbers, and 250 million plus driver history files on individuals. Rolf was sent a written application, He paid the $500 fee. The form wasn't read, for he used two different SSNos on it. And he couldn't disclose M-H's financial information, so he left those spaces blank. After a perfunctory

interview nonetheless he was accepted, and he could peruse the credit files of his colleagues from his own PC. There were individuals credit card nos., SIN nos., addresses, driving records, & credit reports on thousands of businesses. If you asked for credit reports instead of employee reports you would got individuals files. SINs for $20, and added comments about various items cost $15/ each. One bureau gave him credit reports on two colleagues for $20 each; all they needed were their names & addresses. .

Your credit file can travel far and fast, from the original bank, to a credit bureau, to other companies who buy its services. Credit bureaus also buy data from governments, courts, insurance companies. TRW's Financial Lifestyle Database for 10c per name offers mini credit reports with names addresses, phone numbers, credit cards, credit available, income status to any customer: mail order houses, phone / mail marketers, fringe groups. individual names by market segment categories profiles to marketers looking for customers and collection companies... and on and on... Thus businesses can buy the names addresses and phone numbers of most single young women in the Waterloo area who, from their financial, phone, reading and buying habits, and residence, age, etc as determined by based on credit card statements and bank information, etc, would be interested in clothes, records, vacations.

Governments do it too. The RCMP computers track about 25000 people who have not been charged with any crime. No independent watchdog monitors this activity. The US government checked personal records of 11.6 million federal employees against a list of 2.1 million parents behind on their child support payments. While personal privacy is better protected in Canada than in the US, France, Germany or Sweden, it still isn't protected enough. We must tell our SINs to any institution in which we invest our money. Revenue Canada used an employee's income tax return in a disciplinary hearing.

GROUND RULES

Data matching, file building;: If you'll give me the data I'll ask for it; and..
If I can get it, I'll ask for it, whether I need it or not; and,
If I can get it from other sources I'll take that too, until I know you better than you know yourself.

The more liquid the asset the more it approaches info flow in velocity, and the more likely it will become info. Money isn’t money, it's info.. Ditto for investments, stocks, futures, income (our primary possession)

If wealth is property.. and wealth is money and money is info; and it money is certainly more like info than paper (which is also info!). So money flows too, like info; and so do wealth, and property. Wealth is a communicable good (or disease). Privacy is no longer the default, as it is for `real' non-liquid assets, like houses, factories, equipment and workers.
Privacy for one's wealth then has to be bought, eg, in the Caymans, Switzerland, etc.

Information is a commodity. It not only has value, it has economic and indeed monetary value; and perhaps commodities and future markets are information... If you won't give it I'll take it anyways, even if it's unclear or wrong -- Coors workers are polygraphed. Drug testing is required to get hired at some places.. .I have met the enemy and is it us? Or Them? And who is Them? Who is this guy? Businesses, Credit companies, Tax gatherers, the State.

So say no. Dont give information unless you have to and then try to assure that itonly be used for the assigned purpose. Write, given only for use by ---- company for ---- purposes; not to be sold, etc without my consent, or a piece of the action. Pay cash; avoid credit. walk; don’t sign up for

government programs; file no papers with anybody. "live under a rock" Etc And don't let them take it.

In Orwell's 1984 Big Brother was the totalitarian State; in 1994 he'll be the Total Marketer. Leaner employee files. No data, no dossier

SO WHAT'S AN INFORMATION AGE?

It's an age in which information is the prime economic and social good, and the velocity, quantity and efficiency (cheapness) of information flows has increased beyond all expectations and measures, due to rapid and stunning innovations in information and tele-communications technologies (in short, IT).
Also It facilitates interlinking data, forming profiles of individuals surveyed , and they usually can't gain access to such files. This data is often centrally and bureaucratically controlled, sold at great profit with no return to the same individuals, and crosses national borders freely, and is almost totally unregulated by law.

If the measure of an Information Age is the increase of per capita info flow (IF/C) I think *we* are in one, we who live in the advanced OECD and NIC economics; but not the communist or 3d world nations. Ours is the real global village, in the sense that we participate in the Information Age in both the transmitting as well as receiving ends. But in the less developed nations, where the population increases are occurring, most only receive / consume information.

I will therefore merely assume that recent cybernetic and telecommunications technologies, especially when acting together, have significantly increased the per capital info flow, especially in the last decade. This has been reinforced by the rapid increases in transportation flows, and decrease in costs aided by jet planes, fast trains, etc.This has to do with several interlinked factors: technologies, population increases, and the large public and private organizations, urban, state and corporate, based on the previous two.

The technologies are essentially that of the ever larger computer, interlinked in ever more powerful telecommunications networks. They are doing to literate media what Gutenberg's mechanized printing press did to the written manuscript in the 16th century: revolutionizing it. And that communications revolution was not soft; Revolutions swept Europe from 1520s to the 1640s. Today too democratic revolutions are on the rise, with the help of almost instantaneous global info transmission: from Tienanmen Square to Bucharest, to Lithuania, El Salvador and South Africa. The fact that you recognize most? of those names and their significance proves my point. You're connected.

So the Information Age reinforces an old idea: humans like to communicate. Put 2 people together and they will talk; and talk; and talk... Language is the distinguishing mark of the species.

PRIVACY?

But all this has a dark side. The increased flow of information undermines privacy; for privacy is in part the control of information. Privacy is linked to freedom: the freedom not to speak, not to communicate, and the freedom to live one's personal life as one sees fit; ditto for groups like families, institutions like corporations and states. Their freedom too is reinforced by barriers around that information which is specially theirs, which is `privileged'. As *libertas*, it was originally a form of privilege too...

Privacy is a culturally relative notion and difficult to define. For our purposes it relates only to information about oneself. More precisely, it is a constraint on the diffusion of information deemed especially important to one, and whose diffusion would give others more control of one's life, or embarass one, etc. As population and densities increase, the urban megalopolis grows and the need for private spaces, physical and personal, increases. There are great differences in the secrecy of such personal information; in Norway and Sweden all tax information is public.

So the setting for the privacy problem is ironic: the increased information flows of the Information Age in the developed nations, the growth of large modern institutions, organizations, societies; the coming together of peoples in the global village. Increased communication is the problem. In an Information Age, where information moves ever faster and in greater volume at cheaper cost, as do people, and populations grow at perhaps even faster rates, that is, privacy becomes a problem.

The problem is caused by 3 interacting factors, at least:

> Info-telecommunications technologies designed to facilitate information flows,
> Information hungry large organizations, and
> The invisibility or transparency of the first two to those on whom they act.

That is, we are constantly being processed, without our consent or knowledge. Lying at the heart of the privacy problem is another irony: deliberate systemically induced ignorance within the heart of info-telecommunications networks. We need to redesign information technologies in social terms,

SUBVERSION BY INFORMED CONSENT

People have the right to control the communication and use of personal information and to know / control what will be done with it when they volunteer it, whether freely or by law; and to get a cut of any money made from it. How to effect that right is the problem.

This implies that only that data should be required from people by a company of government office that is directly necessary to perform the function, service involved; that data should only be used for the purpose for which it is offered; that data should not be sold or given to third parties without the individual's knowledge and consent and only in the ways they agree to; that data matching, cross linking etc, be similarly constrained as individuals so decide; and finally that individuals have the right and power, at government or company expense, to view their files in toto to ensure their accuracy.

SOME PRIVACY GUIDELINES: THE OECD

The OECD Guideliness offer a model for the responsible handling of such information. They suggest the following general ground rules or pinciples:

> Collection Limits re amounts, and use restricted to the stated purpose, and by informed consent of individuals
>
> Data Quality: data should be accurate, complete and updated.
>
> Purpose Specification: at the time of collection, and use should be limtied to those purposes or others compatible with the original.

Use Limitation: perosnal data should not be disclsoed, etc for purposes other than those specified excet with the subject's consent or by authority of law.

Security Safeguards: to protect data against loss, unauthorized access, modification or disclosure

Openness: re policies, practices regarding use of data; and means to establish existence and nature and use purposes, and identity of controller of data.

Individual Participation: individuals should be able to confirm whether an organization has data relating to him; to have it communicated to him within a reasonable time at reasonable changre, in intelligible form; to be given reasons for denial; to challenge such data

Accountability: organizations controlling data should be accountable for complying with these measures.

While these principles are influential they have not been implemented to constrain state or corporate data collection or use. And given the increases in information flow, and ease of access and search capacity, etc., they are even more urgent that before:

BIBLIOGRAPHY

Archer, L., I saw what you did and I know who you are:" Can. Business, Nov. 1985, 76-83

Brian Bawden and Steen Frandsen, Founation for Responsible Computing. "Mission Statement" and Submission to the National Research Council. Aug., 1989.

Brian Bawden, "The Dependency/Vulnerability Dilemma of Computer and Communications Technology: Ethical and Legal Considerations" Workshop presented Oct., 1989 at U of Guelph World Conference on Ethical Choice in the Age of Pervasive Technology

Forester, Tom, *High-Tech Society*. MIT, 1988., ch. 9.

Forester, Tom, ed., *Computers in the Human Context: IT, Productivity and People*. MIT, 1989. ch. 12, 13.

Garson, B., *The Electronic Sweatshop*. Penguin, 1988., ch. 4, 8, 10.

Herdman, P., "Electronic Monitoring," Position Paper of the Elizabeth Fry Society of Toronto." 27 Oct 89, at U of Guelph World Conference on Ethical Choice in the Age of Pervasive Technology

Irving, Higgins and Safayeni, Computerized Performance Monitoring Systems: Use and Abuse. Communications of the ACM. Aug 1986 29:8 794-801

"Is Nothing Private?" *Business Week*, Sept. 4, 89, Cover Story. 74-82

Hon. Justice Michael Kirby, CMG. "Computers and Privacy- Established Principles: New Problems." 27 Oct 89, at U of Guelph World Conference on Ethical Choice in the Age of Pervasive Technology

Lyon, D. *The Information Society: Issues and Illusions*. (Blackwell, 1988), ch. 5.

R.O. Mason, Four Ethical Issues of the information Age", *MIS Quarterly*. 10:1, Jan 1986. 486-98.

P. Robinsion, chairman of IT workshop. "Ethical Choice in Computers and information Systems." 27 Oct 89, at U of Guelph World Conference on Ethical Choice in the Age of Pervasive Technology

T. Roszak, *The Cult of Information.* Pantheon, 1986, ch. 9.

S. Zuboff, In the Age of the Smart Machine: the future of work and power. Basic, 1988., ch.9, 10,11.

fl\DiNorciaPrivacyinInformationAGE.DOC