The Jurisprudence of Surveillance: A Critical Look at the Laws of Intimacy

Stéphane DESROCHERS(*1) & Alexia ROUSSOS(*2)

***Lex Electronica*, vol. 6, n°2, Hiver / Winter 2001**

Résumé

Affirmer que les citoyens des démocraties occidentales sont l'objet d'une surveillance systématique efficace et à grande échelle a de quoi provoquer une réaction incrédule. Démagogie, diront certains. Pourtant, les progrès réalisés dans les technologies de collecte, de traitement et de stockage d'information forcent une réflexion sur cette hypothèse. Il a été souligné justement que les coûts élevés liés aux moyens rudimentaires employés par les polices secrètes d'antan endiguaient en quelque sorte la menace. Les filatures, les infiltrations, les rapts nocturnes de dissidents pêchaient par manque de subtilité. Au contraire, le génie des techniques modernes vient de ce qu'elles n'entravent pas le quotidien des gens.

Mais au-delà du raffinement technique, le contrôle panoptique de la masse atteint un sommet d'efficience dès lors que celle-ci est amenée à y consentir. Comme le faisait remarquer le professeur Raab : « [TRADUCTION] *La surveillance prospère naturellement dans les régimes autoritaires qui ne s'exposent pas au débat public ni à la critique. Lorsqu'elle est utilisée dans des régimes dits démocratiques, elle est légitimée et circonscrite par des arguments de nécessité ou de justifications spéciales, tout comme la censure* »[1]. Or, le droit, en tant que discours de rationalité, accomplit savamment ce travail de légitimation. C'est dans cet esprit qu'une analyse radicale des règles de droit encadrant le droit à la vie privée apporte une lucidité nouvelle sur notre faux sentiment de sécurité.

Synopsis

To say that the citizens of Western democracies are subjected to systematic surveillance on a wide scale is likely to produce reactions of scepticism. Many would decry this as fear mongering. Notwithstanding, the progress in the technologies of gathering, storing and processing personal data command reflection on such an hypothesis. It has been argued correctly that the high costs related to the rudimentary methods employed by the secret police of old constrained somewhat the threat to privacy. The tailings, infiltrations, and nocturnal abductions of dissidents lacked subtlety. On the contrary, the genius of modern surveillance techniques lies in the fact that they do not disrupt the day to day lives of the persons subjected to them.

Beyond the technical refinements, the panoptic control of the masses achieves maximum efficiency where the subjects can be made to consent to the surveillance. As Professor Raab has noted: "*Surveillance thrives in authoritarian regimes that are not exposed to public debate and criticism. When it is used in political systems that are called democratic, it is legitimized and restricted on grounds of necessity and special justification, as with censorship*"[2]. As a discourse of rationality, the law skilfully accomplishes the task of justification. It is in this mindset that a radical analysis of the laws governing privacy brings a new understanding into our false sense of security.

Table of Contents

Introduction

1. It would seem a bold statement to say that the citizens of Western democracies today are subjected to a higher level of systematic surveillance than were the soviet citizens under Stalin's rule. However, when one considers the size of the population, the territory and the costs inherent to the rudimentary methods used by the KGB to collect, process and record information, there is reason to wonder. That was back in the stone-age of surveillance. Big Brother has gone "high-tech"[3]. Pervasive monitoring devices, invisible to the eye, have brought down the walls that used to guard our intimacy. Consider a recent piece in *Wired* magazine compared the Internet monitoring capabilities of the FSB, Russia's domestic intelligence service, with those of*Doubleclick*[4], an online marketing research firm based in the US. With regards to methods, they appear strikingly similar. The difference is mainly quantitative, with *Doubleclick* reigning supreme[5].

2. Systematic surveillance goes by other names in the West: data mining, marketing research, workplace safety, credit records… all "legitimate" activities. At first glance, there is no reason to be worried. As the right to privacy is becoming a rising concern to employees, consumers and citizens, this essay asks the deeper question of why the threats to privacy have so long been ignored by the general public. Our tentative answer derives from an understanding gained by the Critical Legal Studies (CLS) school of thought about

the role of law in legitimizing social outcomes. We posit from the onset that law and legal theory have contributed to the erosion of whatever privacy there ever was. The essay begins with overview of recurring CLS arguments. We then move to a critique of the classical doctrinal views of the right of privacy, showing that the traditional "rights-based" approach has failed to match strides with galloping privacy-threatening techniques. The following sections present a critical discussion of the laws governing consumer privacy and workplace privacy. The focus of the analysis will be on the many ways that the law formats reasoning along the private/public line, effectively masking the powerlessness of consumers and employees with respect to their privacy.

Critical legal theory and privacy

3. Early CLS writings drew their inspiration from Max Weber's work on the rise of rationality in Western philosophy and in the sociology of law. Weber made the forceful claim that law's appeal to rationality, in conjunction with culture and religion, legitimized the capitalist society. We owe to leftist legal scholars in the United States the spread of his ideas in legal theory. The CLS movement, building on the weberian sociology of law, on Frankfurt School critical theory and on French post-modern philosophy, took the argument of rationality as legitimacy one step further. For CLS scholars, law has historically served to legitimize the domination of the capitalist proprietor. The later outgrowth of the CLS movement were the feminist legal studies (law legitimizing gender-based domination) and the racial legal studies (law legitimizing racial domination).

4. CLS lifted the hood on the inner-workings of legal reasoning as a discourse of conservatism. First, they remarked that law and legal reasoning have traditionally been the staple of white, propertied, bourgeois men. Second, law and legal reasoning create an illusion of determinism; things are the way they are because it is in the natural order of things, and therefore cannot be changed. Third, law and legal reasoning lead to reification, the objectification of reality into neatly defined concepts and hermetically closed categories. Reification holds progressive views in check since they cannot be effectively framed inside the legal construct. For example, the discussion over employee working conditions are contained within the frameworks of contract law and of property law, effectively masking economic inequalities and class struggle (i.e. employee and employer are considered legal entities on equal footing; in his quality of proprietor, the employer can run his factory as he pleases).

5. The highest order of reification is the split that law operates between the private and the public. The private consists of an idealized realm of individual preferences, freedom and unfettered enjoyment of one's property. The public is the realm of state, democratic institutions and political rights. In economic parlance, the split can be explained as one between market allocations and state allocations. CLS scholars see the line separating private and public as indeterminate and, *a fortiori*, political, challenging the view of law as apolitical. The battle over deregulation is illustrative of the politics of law: by choosing to deregulate or to not regulate, the state in effect abandons economic and social outcomes to market forces (private power).

6. Critical legal scholarship has provided powerful theoretical tools to dissect the politics of law. It has been observed that the best CLS literature is applied CLS, that which picks a topic of law and offers a satisfying account of how law in action consistently upholds certain outcomes. The concern of this article is with the laws of privacy. We posit from the onset that law and legal reasoning offer the legitimacy basis for surveillance activities. By creating a vista into the role of law and legal reasoning for the conceptualization of privacy in a technology driven world, certain enduring myths can be exposed. It is only appropriate then to begin the discussion with the theoretical debate concerning the right of privacy.

Privacy vs. surveillance

7. Perhaps the most difficult hurdle to cross when theorizing about privacy lies in the dichotomy between the "rights-based" approach and the "threats approach". The former seeks to find privacy interests in legal doctrines. The later, which we will call, for greater literary effect, the "surveillance approach" is one that seeks to identify activities impacting on privacy. A great deal of scholarly literature can be classified under the rights-based approach, following in the intellectual furrow left by the Warren and Brandeis groundbreaking article The Right to Privacy[6]. The surveillance approach is mostly tributary of the work of journalists and technologists warning of a ubiquitous virtual panopticon, invisibly and systematically gathering, monitoring and recording minute details of our day-to-day lives. Legal scholars, scientifically tied to the method of basing argumentation on existing authorities, have largely followed in the rights-based approach. Until the important paper by Professor Lawrence Lessig, The Architecture of Privacy[7], few have treaded the uncharted waters of the surveillance approach. The relative paucity of scholarly work following in the latter approach may partly explain the widespread claim that regulation protecting privacy has fallen a distance behind the rapid progress of information technologies. Naturally this remark can be understood within the more general intuition that legal reasoning works to stunt efforts to significantly renovate the system in a progressive way.

8. In his paper, Lessig introduced the concepts of the *searchable* and the *monitored*, bringing into light how technology has improved and accelerated surveillance activities, while driving the costs of said activities down. More importantly, Lessig raised the theoretical discussion on privacy one level up by knowingly ignoring the distinction between what could be labeled "active surveillance" and "passive surveillance". By active surveillance we mean those activities which purposely seek to collect, process and record data pertaining to identifiable subjects; by passive surveillance we mean those which systematically and indiscriminately seek to collect, process and record data pertaining to potentially identifiable subjects.

9. Constitutional law is premised on the idea that individual freedoms must be protected against the state. It is unconcerned with the privacy threats originating from the private sector. The constitutions of Canada and the United States both protect citizens against unreasonable searches and seizures by government agents. Searches and seizures are generally construed restrictively as to encompass police actions aimed at identified subjects; they do not cover the systematic recording of personal data by private entities

such as utilities companies. Where the police enter a password to connect to an electrical utility's computer mainframe and examine client accounts for unusual consumption indicative of interior marijuana growing, it is not deemed an unreasonable search[8]. Thus passive surveillance by private entities eludes constitutional safeguards. Now we begin to see how the state (the public) may have relied on the split to spread its antennas below ground in the private. Ultimately the split carries with it the message that the state poses the most serious threats to privacy and freedom, thereby creating a false sense of security when its power is effectively constrained. The split, evident in constitutional law, directs our attention on the "who is watching"; it distracts us from the crucial "why" by implying that watchers fall either in the inoffensive or conspiratorial categories. All watchers have reasons, which, from a privacy standpoint, do not necessarily constitute justification.

10. Doing away with the active/passive distinction underpins the argument that, while active surveillance presents a face seemingly more menacing, passive surveillance is surveillance no less. Active surveillance conjures up images of men in trench coats shadowing dissidents, rummaging through personal effects, kicking down doors and coercing informants KGB style. To be sure passive surveillance lacks such powerful imagery but, in a sense, there lies its greatest threat. Better an evil you know… as the saying goes. In fact it could be asserted that passive surveillance plays into the hands of active surveillance by systematically amassing a wealth of knowledge concerning unsuspecting subjects, knowledge which may abet the dominant forces in perpetuating the totally administered mass society.

11. A critical analysis of the laws of privacy would direct its focus on the role of law in constructing and sustaining this false distinction between active and passive surveillance. As stated above, the analysis will borrow from the CLS tool box and begin summarily to peck away at the reified legal construct which purports to divide the world rationally between the public and the private, and between the active and the passive.

Consumer privacy

12. A good place to start the discussion of the reification of privacy along the private/public divide is precisely where privacy is played out as a subject of public policy. Consumer privacy has attracted much attention lately due to a new awareness of how capabilities in information technology have evolved. Here the private/public paradigm is most obvious because, for the most part of North America[9], comprehensive regulation for the gathering, storage and use of personal data governs the activities of governments but not those of the private sector. Informational privacy practices of consumer outlets are deemed better regulated by the invisible hand of the market. Following economic theory, the market will heed the preferences expressed by consumers and react accordingly, rewarding or punishing good and bad practices. Of course the theory of the market's corrective power rests on the legal tenets of contract law, precisely freedom to contract and its corollary equal standing of contracting parties.

13. CLS literature on the subject of contract law has convincingly showed how these formal tenets serve to conceal the real socio-economic imbalances between market actors[10].

Consumers seldom, if ever, negotiate on a same footing with corporate giants. The markets more often than not present a take it or leave it determination. Therefore consumers have little choice but to waive their right to informational privacy or forego the transaction entirely. It is especially true where the transactions are information sensitive, such as with life insurance contracts, loan agreements or any other contracts involving some form of credit. But aside from these patent cases, economic theory offers a poor explanation for privacy protection when one considers the other elements that can be weighed in any given transaction; price, convenience, lack of information, lack of business savvy can easily downplay privacy as the controlling factor in a transaction.

14. Notwithstanding, the market argument for protecting consumer privacy has supporters even in the legal academia. Professor Lessig himself has expressed the view that laws ought to recognize a property interest in personal data, such that consumers would be empowered in the market and leverage their newfound bargaining power[11]. However, the move toward the *commodification* of personal data does not put to rest the questions raised above. Worse, privacy-as-commodity epitomizes reification in a way that trivializes privacy concerns, lending force to the argument that informational privacy regulation in the private sector is unnecessary.

15. Perhaps the most forceful argument against a market approach to informational privacy is the argument of ethical relativism. Assuming fundamentally that there are no moral essences, the market allocates goods according to individual preferences. It merely aggregates wants and needs, reflecting subjective values. Tying informational privacy to the institution of the market observing a variety of privacy preferences ranging from the unconcerned to the fiercely protective - would forever defuse any claim of informational privacy as a universally human attribute. Prostitution, as an example, offers a convincing illustration of the market's dehumanizing effect. There would be no greater obstacle for those looking to base informational privacy in natural law than the experience of privacy on the auction block.

16. The public/private reification is especially present in the area of consumer privacy. It becomes apparent when one looks at the treatment of consumer databases. Privacy protection in the context of consumer databases does not vary according to property but according to the entity trying to bypass it. Indeed, not all privacy violations are equal. New technologies do not only facilitate the collection and storage of data but also allow for cross-referencing between databases. It is significant in that it makes possible enormous databases with all sorts of information about people, ranging from their race to their revenue, increasing "*(…) the risk of indiscriminate collection, unrelated uses and improper disclosures of personal data*"[12]. That is exactly the kind of database the Canadian government built.

17. In May of 2000, the Privacy Commissioner of Canada made public his annual report. In it, he revealed that the Human Resources Department had created a file that contained information about more than 33 million living and dead Canadians. Each Canadian that had had any contact with any government department was included in the Longitudinal Labour Force File. Some profiles included up to 2,000 pieces of information about the

person. The data collected pertained to date of birth, disabilities, ethnic origin, sex, name, address, education, employment, income and family status. Thus, the Canadian government had in its possession a detailed profile of every one of its citizens that followed their life's evolution. The file was created in 1985 with the purpose of policy research, in this case evaluating the effectiveness of the employment insurance program. The data was compiled from other several other government departments and programs with plans to expand its reach to others like the Canada Student Loan Program.

18. The database raised a number of concerns. The first problem, according to Commissioner Bruce Phillips, is that Canadians didn't know about it[13]. Another problem was its confidentiality. The Human Resources Department claimed that the data in the files was encrypted and that only a few of its employees had access to the decrypted information. Yet it admitted giving the file to private companies for research work. Nothing else was done to secure it from intruders.

19. The file didn't violate provisions of the Privacy Act. Yet it worried the Privacy Commissioner who, while he didn't think that the government was guilty of any abuse, was worried about what future governments could do with the file. He asked for tougher legislation regarding privacy protection. The fact that the compilation was not illegal did not convince Canadian citizens of the legitimacy of the database. They bombarded the Human Resources Development Department with requests for a copy of their files. Provincial governments intervened and asked that the file be destroyed[14]. The public reacted with outrage. So much so that less than two weeks after the news broke, the Human Resources Department announced that it was dismantling the database.

20. Amidst the public outcries and metaphors of "Big Brother", another entity - this time in the private sector - kept on compiling unchallenged even more information on citizens from around the world. Indeed, before there were computers, there was*Equifax*. The company has been compiling information about consumers for more than a century. Since its creation in 1899 under the name Retail Credit, it has been in the consumer credit and insurance claims reporting business. It makes the information it compiles available to other companies that use it to decide if potential clients present credit risks. *Equifax* is where companies turn to whenever they are called upon for a loan, a mortgage or any other kind of credit.

21. In March of 1970, Columbia University Professor Alan Westin, who now heads the Association of Corporate Private Officers formed in July of this year, wrote an article in The New York Times denouncing Retail Credit. He criticized the company for including inaccuracies and rumors in their files on people including "*(...) marital troubles, jobs, school history, childhood, sex life, and political activities*"[15]. He also charged it with not verifying the information it included in the files and with handing the profiles to just about anyone who requested them. At the time, few consumers knew about the existence of such files and even those who did were not permitted to access them. It was only in October 1970, after Westin gave congressional testimony regarding *Equifax* earlier that year, that consumers' right to see the information that was held on them was recognized by way of the Fair Credit Reporting Act.

22. *Equifax* receives its information on consumers from companies that provide them credit or loans. Such companies can be banks, credit card companies, retailers and collection agencies. Claims are not verified. Thus even litigious claims can be added to a file. For example, if you do not pay for an iron, it will be added to your file even though you refused to pay for it because it never functioned. Other mistakes can appear in your file like a loan that you've already paid or somebody else's loan appearing in your file. The information contained in the file remains there generally for 7 to 10 years. Unless the consumer corrects this information, it stays there for that period of time.

23. Consumers can ask for a copy of their files for 8$. Only when they have it in hand along with the order confirmation number will *Equifax* discuss the information in the file. Once a consumer files a dispute, it is reviewed and considered by *Equifax*. If it does not solve the dispute, the complaint is sent to the relevant creditor. The file is then modified or not, according to the creditor's comments. If the consumer still isn't satisfied, he can send a statement not exceeding 100 words that will be added to his file. The paragraph being longer than 100 words, it is obvious that the creditor has the last word in these disputes. Thus, while consumers can access their files and report mistakes, most of them do not. For those who do, there is not a guarantee that the information will be corrected.

24. In 1995, a new wave of concern about *Equifax* hit privacy advocates. At the time, the company was making headway in the medical reporting business. It owned a subsidiary that employed paramedics who did medical exams for insurance companies and purchased Osborn laboratories, a company that did medical test result analysis. The biggest problem was that it announced it was pairing up with AT&T to offer medical records "storage", a centralized system in which every American's medical record would be available for any doctor to view or download. While the system was never introduced, *Equifax* today collaborates with other companies like *Medicheck Services Inc.* and *ENVOY* to give healthcare providers "*(...) patient identification verification and financial information services (...)*"[16] therefore helping providers to get "*(...) payment for services after discharge*"[17].

25. *Equifax* holds *"(...) private and personal information on just about every man, woman and child in the United States, which is sold as widely as possible to make money*"[18]. Some of the people who can see credit files are employers, credit grantors like banks and credit card companies, collection agencies and insurance companies. If the data about a person is wrong, he may never get a house, a car or even a job. And yet, *Equifax* has been functioning for over a century. There haven't been any outcries like there were for the Canadian Human Resources Department, the few who have been watching the company and denouncing its actions have been privacy activists.

Employee privacy

26. Much CLS literature has focused its aim at employment law and labour relations[19]. Here the law has served to institutionalize the relation of obedience to the employer. Faced with economic necessity, employees are nevertheless deemed by the law to have freely "consented" to being ruled inside the factory by its proprietor.

27. Employees are routinely asked to sacrifice privacy rights to managerial interests like efficient recruitment, productivity, liability risks and prevention of theft. While it has been observed that the workplace is "*especially suited for social intercourse*"[20], the outright negation of privacy at work prevents free expression and human fulfillment. In a progressive mindset, computer networks in the workplace could be envisaged as a powerful means of creating solidarities and accelerating unionization of workers in precarious situations. Instead courts have insisted on property rights, affirming the principle that employers may police communications taking place inside their premises with the use of their equipment. As a result, surreptitious surveillance of Internet and email activities by employers has become commonplace and has produced the handy pretexts for dismissing personnel. In addition to the divine rights accruing from ownership of the networks, employers' predictably invoke such compelling legal grounds as the need to filter email to shield employees from sexual harassment, or abusive language or even threats.

28. The response has been to devise regulation forcing employers to disclose beforehand their monitoring policies. Apparently the fundamental tenets of justice require that the subjects of eavesdropping be forewarned of this possibility. All is good and well then. Of course, this is just another twist on the "consent" theory, aligned with the view that a "delinquent" employee has but himself to blame if he is caught wasting company time or causing strain on valuable computer resources. The employee is therefore "responsibilized" into submission, forgetting what dignity is usually owed to him away from the office.

29. Giving prior notice of the possibility of conducting surveillance activities is deemed a fair practice. What is purposely omitted in the equation is the fact that privacy is negated altogether. Thinking of reclaiming the right of privacy cannot even be entertained. The panoptic effect is achieved. Instilled with the subjective belief that they are constantly being watched, regardless of whether it is true, employees develop a sense of paranoia. In time the feeling gives way to a sort of programmed cautiousness. The employees know that they can never be free during office hours, but accept this as a mild fatality. We begin to confuse speaking privately with acting secretively, becoming more and more self-conscious with the idea of doing something wrong. In a way, the factory or the office act as a training ground for learned powerlessness in a larger perspective.

30. The right of employers to survey their employees is jeopardizing the right to privacy of employees. According to an April 2000 survey by the American Management Association, 73 percent of large American companies monitor their employees' email, computer files, Internet connections or telephone calls, twice the number revealed in the 1997 edition of the study[21]. Although employee surveillance is by no means a new phenomenon, the possibility to do so without any human intervention or interruption is. New technologies abet employers in their pursuit of the utmost productivity. When the technology coincides with the economic justification, why hesitate?

31. In some industries, employees are constantly monitored. Their telephone conversations are listened to and recorded, their sixty minutes of lunch are calculated by their headsets, the same is done for their maximum of twelve minutes of breaks a day[22]. In other workplaces, employees' every moves are recorded by camera. Other employees are

routinely submitted to unwarranted drug tests. These tests are administered as part of the recruitment interview but also during the course of employment. Of course, employees may refuse to submit themselves to the test. It is their body after all and they are entitled to their integrity. They are equal to the employer and may simply refuse and contact another company for a job, right? What's next, genetic testing? Wrong, the future is now it seems. Citing a study conducted in the last year, the Electronic Privacy Information Center and Privacy International indicate that "*(...) 15 percent of major U.S. firms are conducting some kind of genetic testing or "testing for susceptibility to workplace hazards"*.", quite an increase from the 1.6 percent who were doing so in 1989[23].

32. However, genetic testing is far from being as popular as email[24] and Internet use monitoring. Most people today know that their email at work is or can be monitored. The courts have generally condoned this behavior. The general argument is that the employer owns the computer, pays for the connection to the Internet and gives the employee an email account for business purposes. Additional arguments are that the employer has a legitimate interest in verifying that his employees are productive, that they do not divulge trade secrets, that they do not transmit inappropriate material, for which he could eventually be liable[25], and that the company servers are not overloaded. Yet another reason given is that employees do not have any expectancy of privacy since they know that it is possible for other people to read their email.

33. To this day, no Canadian court has had to decide a case concerning the subject. In the United States however, some decisions are now famous. The first one, *Smyth* v. *Pillsbury*[26], concerned a former regional operations manager's claim that he had been wrongfully dismissed. Pillsbury had given its employees access to email accounts to facilitate communication within the company. It had told them repeatedly that their messages would not be monitored, that their privacy would be respected. Moreover, it had said that "*e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand*". The plaintiff was told this personally. Yet, the messages he sent to his supervisor were read and were used as the basis for his dismissal. He was discharged for having sent messages containing "*inappropriate and unprofessional comments over [the company's] e-mail system*". According to the judge, once Smyth had sent his comments on his employer's e-mail system, which was used by everyone in the company, he had no reasonable expectation of privacy notwithstanding his employer's assurances that his messages would be confidential. The judge also noted that even if the plaintiff's privacy interests were at stake, "*a reasonable person would [not] consider the defendant's interception of [the] communications to be a substantial and highly offensive invasion of [the plaintiff's] privacy*", and that the employer's interest in "*preventing inappropriate and unprofessional comments or illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments*".

34. Another recent case comes to us from the Texas Court of Appeals. In *McLaren* v. *Microsoft*[27], McLaren accused Microsoft of having invaded his privacy by accessing and distributing the email stored in his personal folder on his computer. McLaren had been suspended pending an investigation following accusations of sexual

harassment and "inventory questions". He informed his employer that he wanted to access his personal folder because it contained email messages regarding the accusations against him. Microsoft read his emails and fired him based on their contents. According to the judges, McLaren did not have a reasonable expectation of privacy since the emails were transmitted over the company's network and were "*at some point accessible to a third-party*". They noted that notwithstanding the personal password he used to access his messages and the fact he stored them in his "personal folder", the messages "*were not McLaren's personal property, but were merely an inherent part of the office environment*". Moreover, they concluded that even if McLaren had a reasonable expectation of privacy, "*a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion*". Citing *Smyth*v. *Pillsbury*[28], the Court found that the employers "*interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh McLarens's claimed privacy interest in those communications*".

35. Beyond the employee's privacy, it is his dignity that is being jeopardized. While American courts have been slow in recognizing the problem, generally siding with the employer, the government recently introduced legislation, which would ban any monitoring done by employers without notice to employees[29]. If adopted, this law would oblige employers to reveal to their workers that they will be monitored. They would have to tell all new employees when hiring them and give notice to all employees once a year and in case of a change in the monitoring policy. It is probable that employers would not get away with vague notification nor with implicit consent since the bill requires that the notice be clear and describe the form of activity that will be monitored, the means by which it will be accomplished, the kinds of information that will be obtained, the frequency of monitoring and how the information will be stored and used.

36. The bill does not prohibit surveillance in any way, doesn't require that employees be informed every time they are monitored and permits secret monitoring when the employer has reason to believe that the worker is harming either other employees or the company. Although not very restrictive, it goes a long way in protecting employees' dignity.

Conclusion

37. The idea behind this text was not to dig deep into the Laws of privacy and expose their tenets. The motivation behind this text was to expose not only the current threats to privacy by employers and databases, but the biggest threat of all, the false sense of security engineered by the reified legal construct. The idea that the right to privacy is safe because government action is subject to legal constraints is deceiving. Likewise, privately held databases pose a serious threat to privacy. Corporations should be held accountable no less for there actions simply because the law categorizes them as private entities. In *The Fountainhead*[30], the ultraconservative Ayn Rand wrote: "*Civilization is the progress of a society toward privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from man*"[31]. More and more we are witnessing the disappearance of this "privacy". As this is happening, we are losing all possibilities for second chances. Should a person not be able to get a second job because

he didn't do well with his first employer? And what if that first employer didn't give him a first chance?

38. We find ourselves more and more having to distinguish between what is private and what is secret, a distinction we never had to make before. In an age when deleted email messages can be found many years later, this distinction, unless limited by appropriate legislation, could be part of our daily lives. Privacy is not simply where you are and what you're doing. It has not only to do with "I have nothing to hide…" nor with "If it can save me when I'm unconscious in a hospital…". It has to do with freedom, individuality and dignity.

39. "*Privacy is related entirely to the degree to which we respect each other as unique individuals, each with our own sets of values which we are entitled to make known or not as we see fit. To truly respect your neighbour, you must grant that person a private life. Respecting one another's privacy means the difference between a life of liberty, autonomy and dignity, and a hollow and intimidating existence under a cloud of constant oppressive surveillance*"[32].

Notes

(*1) Avocat, Assistant de recherche au Centre de recherche de droit public, étudiant à la Maîtrise « Droit des technologies de l'information » de l'Université de Montréal (Canada Qc). Email : solanie@supernet.ca.

(*2) Avocate, Assistante de recherche au Centre de recherche de droit public, étudiante à la Maîtrise « Droit des technologies de l'information » de l'Université de Montréal (Canada Qc). Email : roussa@lexum.umontreal.ca.

[1] C. Raab, "Connecting Orwell to Athens? Information Superhighways and the Privacy Debate", in W.B.H.J. Van de Donk et al., *Orwell in Athens*, Amsterdam, *IOS Press*, 1995, p. 209.

[2] See C. Raab, *supra*.

[3] D. Banisar, "Big Brother Goes High-Tech", at <http://www.networkusa.org/fingerprint/page3/fp-big-brother-high-tech.html>.

[4] T. McNichol, "Double Agents", *Wired* No. 8.06, June 2000, p. 124.

[5] Interestingly, the table indicates that *Doubleclick* overwhelmingly wins the numbers battle, having recorded data on 88 million American households compared with the FSB's 5 million Russian users.

[6] S.D. Warren & L.D. Brandeis, "The Right to Privacy", *Harvard Law Journal*, 1890, Vol. 4, 193.

[7] L. Lessig, "The Architecture of Privacy", at <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf:>

[8] *R* v. *Plant*, [1993] 3 *S.C.R.* 281.

[9] The province of Quebec has passed a comprehensive law regulating informational privacy practices in the private sector.

[10] For an illustration of the CLS critique of contract law see P. Gabel & J. Feinman, "Contract Law as Ideology", in D. Kairys, *The Politics of Law*, New York, Pantheon Books, 1982, p. 172.

[11] See *supra* note 2, p. 17. Professor Lessig posits that a property regime would enable consumers to "hold out" until an acceptable price is offered, effectively offsetting the low costs of monitoring and searching.

[12] Privacy Commissioner of Canada, "Annual Report 1999-2000", May 2000, <http://www.privcom.gc.ca/english/02_04_08_e.htm>.

[13] Although the database was mentioned on the Human Resources Department website, it was not enough notice for Canadians to be aware of it. Even the Privacy Commissioners were not aware of its existence. Indeed they had repeatedly reassured Canadians that "*(...) there was no single federal government file, or profile about them*", *Idem*.

[14] Truth be told, while provincial governments strongly criticized the federal government's database, they are not without reproach. The *Ministère du Revenu du Québec*, for instance, is known to cross-reference its files with those of many other departments, including electricity bills, in its fight against tax evasion. See G. Nadeau, "Surprise! Québec a aussi son mégafichier", *Multimédium*, 13 June 2000, <http://www.mmedium.com/dossiers/bigbrother/4.html>, referring to *Ministère du Revenu du Québec*, "Rapport d'activité résultant de la comparaison, du couplage ou de l'appariement des fichiers de renseignements au 31 mars 1999", 31 March 1999, <http://www1.revenu.gouv.qc.ca/MRQWF5F.PDF>.

[15] Quoted in Simson Garfinkel, "Separating Equifax from Fiction", *Wired*, September 1995, <http://www.wirednews.com/wired/archive/3.09/equifax_pr.html>.

[16] Equifax, "Equifax signs agreement with Medicheck Services Inc.", Press Release, December 30, 1998. <http://www.equifax.com/about/news_releases/december98/nrefxmedick.html>.

[17] Equifax, "Equifax and Envoy to facilitate decisions by healthcare providers ", Press Release, November 23, 1998. <http://www.equifax.com/about/news_releases/november98/nrefxenvoy.html>.

[18] Simson Garfinkel, *op. cit.*, note 15.

[19] See R. Austin, "Employer Abuse, Worker Resistance, and the Tort of Intentional Infliction of Emotional Distress", *Stanford Law Review*, Vol. 41, 1988, p.1.; K.E. Klare, "Critical Theory and Labor Relations Law", in D. Kairys, *The Politics of Law*, Pantheon Books, 1982, New York, p. 65

[20] *Idem.*, p. 65.

[21] American Management Association, *2000 AMA Survey: Workplace Monitoring & Surveillance*, April 2000, <http://www.amanet.org/research/stats.htm>.

[22] Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2000: an International Survey of Privacy Laws and Developments*, <http://www.privacyinternational.org/survey/phr2000/threats.html#Heading18>.

[23] *Idem*.

[24] On the nature of email, we refer the reader to René Pépin, "Le statut juridique du courriel au Canada et aux États-Unis", *Lex Electronica*, vol. 6, nº 2, winter 2001.

[25] For some people, sending inappropriate jokes or comments via company email is the equivalent of doing it on company letterhead.

[26] *Smyth* v. *Pillsbury*, 914 F. Supp. 97, 101 (E.D. Pa. 1996). A copy can be found at <http://www.loundy.com/CASES/Smyth_v_Pillsbury.html>

[27] *McLaren* v. *Microsoft*, 1999 WL 339015 (Tex. App. 1999). A copy can be found at <http://www.bna.com/e-law/cases/mclaren.html>.

[28] *Op. cit.*, note 26.

[29] The *Notice of Electronic Monitoring Act*, (S.2898 and H.R.4908), introduced July 20, 2000. A copy can be found at <http://thomas.loc.gov/cgi-bin/query/z?c106:HR.4908:>.

[30] Ayn Rand, *The Fountainhead*, 1943.

[31] We are not hereby endorsing Mrs. Rand's philosophy. Nonetheless, we think that this quote illustrates well the need to preserve privacy. Privacy, it seems, is an issue that can bring together both the conservative and progressive sides.

[32] Bruce Phillips, Privacy Commissioner of Canada, 1999.