INFORMATION TECHNOLOGY AND WORKERS' PRIVACY: NOTICE AND CONSENT

Roberto Fragale Filho† and Mark Jeffery††

I. INTRODUCTION

The concepts of notice and consent are quite distinct and yet they are often very closely interconnected. For our present purposes, "notice" may be defined as the employer's communication to the workers involved (or their representatives) of the workplace policies or practices related to surveillance or data processing; and "consent" may be defined as a positive expression of agreement by those workers (or possibly their representatives) to the surveillance or processing described in the notice. The close relation between the two concepts is immediately clear: for obviously, consent can only be given if the person who gives it has first been notified of what he or she is being asked to consent to. But it is no less clear that there are important differences between the two: Above all, notice is passive: employees receive information; but consent is active: workers must respond to that information. Thus, notice should result in all parties having a clear understanding of the conditions under which the employer expects the employees to work; whereas consent, in addition to this function of clarification, should also mean that the workers concerned have exercised an explicit choice over whether or not to accept these conditions.

Despite these differences, the two concepts are sometimes conflated (or simply confused), most especially in the way that notice may be taken to be equivalent to consent. In the context of employment, this conflation has its roots in the classical, "liberal" conception of the employment contract, which was well expressed by a New York trial court in 1890:

† Professor de Direito, Federal Fluminese University, Niterói, and Labor Judge, Rio de Janeiro, Brazil.

†† Professor de Dret, Open University of Catalonia, Barcelona, Spain.

> It is the right of the employer to establish rules. If a workman, on seeing these rules, is dissatisfied with them, he need not accept the employment. If he accepts it, however, he must obey the rules. If he disobeys the rules, he breaks his part of the contract, because it is a part of the contract to obey them.[1]

According to this perspective, once employees or candidates have been notified of the "rules"—in our case, of the surveillance and processing of personal data that the employer intends to implement—they may then decide whether they wish to work under these conditions. If they do not, they are free to leave the job or to choose not to accept an offer.

Some thinkers follow this proposition with a further step, arguing that where an employee is given notice of surveillance or processing and continues to work, this failure to leave the job means that he or she has given "implied" consent. Whether or not one accepts this interpretation depends upon the extent to which one takes consent to imply a free choice—and, indeed, upon whether one focuses on contract theory or social and economic realities. In practice, this kind of choice may depend heavily on whether suitable alternative employment is readily available: if there are risks, difficulties, or inconveniences in finding an alternative job, then workers may be forced to conclude that these considerations are more important than any unwelcome intrusions into their private lives. Moreover, the concept of "implied consent" itself surely confuses acquiescence—passively accepting a situation whether one likes it or not—with consent, which implies a real choice and an active acceptance. In questions such as those relating to surveillance at work, and to the processing of employees' personal data, the law might do well to maintain this distinction, given that the privacy and human dignity of citizens may be at stake.

In the following discussion, we shall keep in mind the links between the two concepts, but with the hope of presenting our analysis more clearly, we shall examine them separately.

II. NOTICE

A certain loss of freedom is an inevitable and accepted part of the employment relationship. As with any contract, individuals accept obligations toward one another and these obligations may then have the effect of limiting the scope of the rights and freedoms that those individuals enjoy as citizens. Such limitations may be acceptable to

1. Forsyth v. McKinney, 8 N.Y.S. 561 (Sup. Ct. 1890).

the law because the surrender of these rights and freedoms is the result of a free choice by the person who holds them, and because they may be restored to that person at any time simply by ending the contract. This would explain the fact that, although in all of the countries that we looked at in this project, there are laws that guarantee some aspects of individuals' privacy or dignity, employers nevertheless enjoy a considerable margin of discretion when it comes to deciding whether and how they will conduct surveillance of their employees and whether and how they will process personal data about them. Indeed, it is both socially and legally accepted in all of these countries that some degree of surveillance and data processing is necessary in all employment relationships.[2]

Nonetheless, the national studies also show that there is a very widespread expectation that any surveillance of workers should be done in a clear and open manner, and thus a widespread expectation that employers will notify the workers of all such practices. There are a number of possible explanations for this expectation of openness. First, following the classical, contractual analysis of the employment relationship (and quite apart from any considerations of employment rights and human rights), if the employer is going to "set the rules" and the worker is then going to choose whether or not to accept the job on the basis of those rules, then clearly, in order to make that choice, each worker must be fully informed of all the conditions of employment. Secret practices make it impossible for employees to take an informed decision and so undermine the analysis itself. Second, the law may imply a general term into all employment contracts, according to which the parties must act in good faith or show loyalty to one another: undeclared surveillance may well be considered incompatible with such a condition. And this leads on to the third, and most general, of the possible explanations. It may be that the secret surveillance of employees is socially unacceptable—it may be seen as sneaky, underhanded, unfair, devious, or even sinister. Such considerations have now become all the more important, because the use of new information technologies permits employers to conduct surveillance which, while being ever more intrusive, is ever less perceptible.

Questions of what is and is not socially acceptable may also explain why the expectation of openness centers on the surveillance of workers—which may be taken to be "spying" upon them—and does

2. *See* Mark Jeffery, *Information Technology and Workers' Privacy: Introduction*, 23 COMP. LAB. L. & POL'Y J. 251 (2002).

not generally include the processing of personal data about workers, which is perhaps seen as nothing more than bureaucratic record-keeping, and so does not tend to excite such controversy. Indeed, in countries such as Brazil and the United States, surveillance and the processing of personal data are seen as two distinct areas, and so a difference in the approach of the law toward the two may be maintained. In the Member States of the European Union, however, it is clear that the definition of "processing of personal data" set out in Article 2 of Directive 95/46/EC also covers all forms of computer surveillance, and so both areas come under the same rules. Thus, for example, the fact that the Directive requires all processing of personal data to be done "fairly" means that if secret surveillance is considered unfair, it will also be unlawful. A similar reading may be made of the International Labour Organization, (ILO) *Code of Practice on the Protection of Workers' Personal Data*.[3]

A. Legal Requirements to Notify

The Member States of the European Union show some differences over the question of whether there is a legal requirement to notify workers of surveillance. In the French Labour Code, there is a clear requirement for prior notification before the collection of any information about employees; but in most other countries, the requirement is implicit—for example, in the German requirement to notify the Works Council of the installation of new surveillance equipment and in the Spanish prohibition on fraudulent, unfair, and unlawful monitoring. In Britain, there is a specific legal requirement to have consent before intercepting messages on any telecommunications system, but this general position is now unclear in cases of employment, following the creation of (ill-defined) exceptions for businesses. All laws in the Member States are, however, subject to the overriding requirements of Directive 95/46/EC, according to which all data subjects must be given information about the nature of all personal data held about them (unless they themselves provided the data) and must be informed of the identity of the data processor, of the purpose of the processing, of their rights to access and rectify data, and of any other information necessary in the circumstances in order

3. Directive 95/46/EC, arts. 2(a), (b) & 6(1)(a) (EU); Code of Practice on the Protection of Worker's Personal Data, ¶¶ 3.1, 3.2, 5.1 (ILO). In terms of the overlap between surveillance and processing, it is interesting to note that both the Directive and the Code create different rules, according to whether the personal data were obtained from the data subject/worker or from third parties or other sources. It is then perhaps not entirely clear which set of rules would apply to personal data obtained through secret computer surveillance of the data subject.

to make the processing fair. Thus, throughout the European Union, there is now a legal duty upon employers to notify all workers of any surveillance or any processing of their personal data.[4]

By contrast, in the United States and Brazil, there are relatively few direct legal obligations to notify workers; and those that do exist tend to be concerned with surveillance rather than data processing. In the United States, there is federal legislation that creates (somewhat limited) protection against the interception of communications, but this may be avoided where the parties to the communication have given their consent, and the courts have taken this to include "implied consent"—so, in effect, all employers are required to do so in order to make a lawful interception is to give notice of it. Only two states (Connecticut and Delaware) require that employees be informed of electronic monitoring. Yet despite this lack of legislation, a survey—cited in Matthew W. Finkin's report on the U.S. law—found that 88% of U.S. employers notify their employees of the electronic monitoring to which they are subjected.[5] It is certainly possible that this very high level of notification relates to the importance that employers give to clarity and free choice in the operation of their employment relations, or to their repugnance of secret surveillance. However, it seems most likely to relate to an indirect legal requirement to notify. As we shall see below, if workers in the United States are notified of surveillance, this may, for the purposes of the law, put an end to any reasonable expectation of privacy that they may have had. Consequently, they may no longer have any grounds to sue their employer for a wrongful invasion of their privacy arising from that surveillance. In Brazil, there are no statutory requirements to notify workers of surveillance, but the labor courts have a general power to assess the reasonableness of an employer's actions and this, coupled with the constitutional guarantee of privacy (and perhaps also the feeling that secret surveillance is socially unacceptable), may give rise to a general presumption that employers should give such notification.

B. Mechanisms for Notification

Where notification is required by the law, different mechanisms may be envisaged. For example, with respect to the person or persons to whom the notice must be addressed, some laws permit a collective

4. *See* DIRECTIVE 95/46/EC, *supra* note 3, at arts. 10, 11 (EU). This duty is, of course, subject to the (limited) exceptions set out in the Directive.

5. Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471 (2002).

form of notification. Thus, the law of Connecticut allows notification to be made by means of a poster displayed at the workplace; and the requirements of the German law on surveillance may be satisfied by a general notification. Moreover, even though the notification requirements of Directive 95/46/EC make specific reference to the provision of information to the data subject, in cases where the same information would satisfy the requirement with respect to a number of data subjects, there would seem to be no reason why the subjects could not be informed as a group. Indeed, the Directive specifically states that its notification requirements only apply where the data subject does not already have the information in question; so, where all the requisite information has already been provided—by whatever means, collective or individual—then these requirements will be satisfied.[6] Some national laws—such as those of France, Germany, and Spain—also require that the workers' representatives be notified of the surveillance or processing (or at least of the installation of equipment that may be used for these purposes).[7] The creation of such laws is encouraged in the ILO Code of Practice and in the Council of Europe's *Recommendation R(89)2 on the Protection of Personal Data used for Employment Purposes*.[8]

By contrast, the law rarely specifies the form that the notification should take. It generally makes sense to give notice in written form, if only because the very purpose of notification is to ensure that it is clear that the employees know that surveillance and processing may take place. Oral notice does not provide such clarity, as there is no proof as to what information was communicated and as the parties may disagree in their recollections of this. Nonetheless, even written notice may sometimes fail to provide the necessary clarity. For example, a poster such as that envisaged by the Connecticut law may give rise to doubts over whether or not it was sited prominently

6. *See* DIRECTIVE 95/46/EC, *supra* note 3, at arts. 2(h), 10, 11. Similarly, where the condition of consent is being relied upon by the employer (see below), then the Directive's requirement in Article 2(h) that consent be the result of an "informed" decision by the data subject does not necessarily imply that the information has to be provided on an individual basis, although it may require a mechanism for ensuring that each individual worker has received and understood the collectively-addressed information.

7. In the United States, surveillance of employees is a working condition that must be negotiated with a union. National Steel Corp. v. NLRB, 324 F.3d 928 (7th Cir. 2003). But only about 9% of the civilian workforce is represented by unions.

8. *See* Code of Practice on the Protection of Workers' Personal Data, *supra* note 3, ¶ 12.2 (ILO) referring to the consultation of workers' representatives over the installation of systems for processing and surveillance; Recommendation R(89)d on the Protection of Personal Data Used for Employment Purposes, ¶ 3.1 (Council of Europe) (making a more general call for employees or their representatives to be informed or consulted about processing or surveillance).

enough for a particular employee to have been aware of it; and all forms of written notice may be subject to doubts about whether the wording used and the language in which it was written were such that a particular employee could reasonably be expected to have understood it. But these doubts notwithstanding, employers would generally be advised to give notice in written form in order to make the situation as clear as possible. This conclusion makes the legal situation in Italy all the more curious: the one country in our study with a general requirement that notice be in written form created a specific exception to this rule in the case of employment. Ostensibly, this was for "business" reasons—to prevent enterprises from being overloaded with bureaucratic requirements—but there is now clearly a possibility (whether unintentionally created or otherwise) that the law on data protection will become less effective in practice. Whatever the short-term advantages of oral notification may be for Italian employers, they would surely be wise to renounce these in favor of the longer-term advantage of clearly establishing whether and to what extent their employees know that they might be subject to surveillance and might have their personal data processed.

C. The Legal Effects of Notification

The fact of notification does not in itself legalize any and all practices by employers; in many cases, there remain legal limits upon surveillance and upon the processing of personal data. In general, the giving of notice should simply establish clearly that a particular employee has been warned about the surveillance or processing that the employer might undertake. This may then have further legal consequences.

One such consequence may be to affect the recognition by the law of any expectations of privacy that the employee may have had. This position in clearest in the United States, where such protection as is afforded by the tort of invasion of privacy is not available to employees if they have been notified of the possibility of surveillance. According to this law, once notice has been given, an employee cannot reasonably expect any privacy and so there can be no question of wrongful harm. The very opposite position has been taken in France, where the highest appeal court has ruled that the expectation of privacy (at least, as regards the secrecy of communications) can never be over-ridden: Employees may be disciplined if, having been notified of a prohibition on the private use of their employer's computer facilities, they then disobey this rule; but the legal

protection of privacy remains unaffected, and so the employer may not examine the contents of any private files sent or stored in breach of the prohibition. Courts in Brazil might be expected to take a similarly robust line (in the interpretation of the constitutional provisions on the secrecy of communications); and courts in Britain, Germany, and Spain might perhaps fall between the two extremes: Notification of a prohibition on private use would certainly make it lawful for an employer to conduct surveillance in order to enforce that prohibition, but the extent to which employers could examine the contents of communications as part of this enforcement remains to be defined.[9]

Another consequence of notice may be the fulfillment of a statutory requirement that workers give their consent to certain forms of surveillance or data processing. As we have already noted, courts in the United States have held that "implied consent" (that is, notice) will suffice for the federal and state legislation which prohibits the interception of communications unless the interlocutors have consented.

Notice may also have the effect of setting limits on the extent to which employers may conduct surveillance and process personal data. If the employer permits the private use of the company's communications facilities, then, unless they are notified to the contrary, employees may have a legitimate expectation that the privacy of their communications will be respected and so it may be unlawful for the employer to examine the contents of any such messages. This would certainly seem to be the case in the EU Member States, with their general legal requirement of fairness in all data processing; and also in Brazil, where the labor courts would

9. The attitude of the European Court of Human Rights is, unfortunately, somewhat ambiguous in this area. Comments made in the case of Halford v. U.K. would seem to imply that the giving of notice will affect the scope of the application of the right to have one's private life respected (as established by Article 8 of the European Convention on Human Rights). Halford v. U.K., 24 E.H.R.R. 523 9ECHR 1997) (Case 73/1996/692/884, *available at* http://www.echr.coe.int). However, no further indication was given of the extent to which notice might affect this right, and the comments are in contrast to the much wider application of Article 8 to employment relations that was taken in the earlier case of Niemitz v. Germany. Niemitz v. Germany, 16 E.H.R.R. 97 (ECHR 1991) (Case 72/1991/324/396, *available at* http://www.echr.coe.int). The European Union's independent committee of experts on data protection is of the opinion that, whatever the effect of the comments in Halford might be on the European Convention of Human Rights, notice from the employer will not affect any of the data protection rights enjoyed by workers under Directive 95/46/EC. Article 29 Data Protection Working Party, "Working Document on the Surveillance of Electronic Communications in the Workplace," EU Document No. 5401/01/EC/Final, WP55 (May 29, 2002). *See also* M. Ford, *Two Conceptions of Worker Privacy*, 31 INDUS. L.J. 135 (2002) (arguing that, in the application of the Convention to national law, courts in the United Kingdom are likely to favor a wider approach and thus to limit the effect of notice).

probably hold such interception to be unreasonable. Moreover, once notice has been given—once the employees have been led to expect that surveillance and processing might occur in the circumstances stated in the notice, but not in any others—it could well seem unfair and unreasonable for the employer to exceed these limits. So any practices that go beyond what was set out in the employer's notice may also be held to be unlawful. Again, the United States provides an opposing example: It would seem that employees cannot even rely on the common law remedies for deceit where an employer deliberately misleads them as to the nature and extent of the surveillance to which they will be subjected.

Further legal consequences may arise if the notice alters the terms of the contract of employment. Where the notice is nothing more than a memorandum—that is, where it says how the rules in the contract are to be applied, but does not alter the rules themselves—then its legal effects may be limited; but where it establishes new and binding rules, then this may constitute an alteration of the terms of the employment contract,[10] and so bring with it questions over the employer's ability to make such changes in a unilateral manner. In some countries, such changes may also affect questions of collective labor law. In France, for example, the law requires that the Works Council be consulted before the introduction of any new company rules that are backed up with disciplinary sanctions.

Last, we should note that the legal consequences of notice may be affected if there are discrepancies between the employer's policy as set out in that notice and the actual policy that the employer puts into practice. Where employers give notice which defines certain limits, but then go on to ignore those limits, the law in most of the countries studied in this project would consider that the subsequent practice had led to the establishment of a *de facto* policy which supersedes the policy set out in the notice. So, for example, where the notice prohibits the private use of company communications facilities, this may have an important influence upon the extent to which the law will accept the surveillance of private communications; but if in practice the employer tolerates such private use, then this will create a *de facto* policy that may override the notice—and this may in turn mean that the law will not permit the forms of surveillance specified in that notice. In this case, the employer's practice alters the employees'

10. Most courts in the United States, for example, consider employee manuals, handbooks, and company codes of conduct to be legally-binding, so changes to them could affect the contractual relationship between employer and employee.

reasonable expectations of privacy, and so, once again, it would be unfair (or in bad faith, or disloyal) to go against these expectations. The employer would have to give new notice before enforcing any policy that is more restrictive than that which operates in practice. Once again, an alternative perspective predominates in the United States, where the original notice destroys once-and-for-all any expectations of privacy that the employee might have had. Nevertheless, U.S. employers who have an official policy which involves an invasion of their employee's privacy—such as random personal searches—may be advised to make occasional searches, if for no other reason than to ensure that the policy remains "active" and that the employees do not have any opportunity to develop a reasonable expectation of privacy.

III. CONSENT

Two different situations may be envisaged in which workers may be asked to consent to surveillance at work and to the processing of their personal data. First, consent may be given as part of the contract of employment. We have already argued that the operation of a contract of employment will almost inevitably oblige workers to agree to the limitation of some of the rights and freedoms that they enjoy as citizens: employees expressly or implicitly consent to being subjected to a certain degree of control by their employer. This agreement will probably cover the controls necessary to ensure that employees do their job safely and in accordance with their contractual obligations. Whether and to what extent it covers other forms of surveillance and data processing is a much more complicated question, which requires a balance to be set between employers' rights to run their businesses and employees' rights to privacy.[11]

Second, consent may be given (whether in a contract of employment or in some other form) in response to legislation that expressly forbids employers to engage in certain practices unless they have obtained the consent of the workers involved. For example, the legislation on data processing in the European Union and in a handful of U.S. states sets out a number of circumstances in which the processing of personal data may be lawful, and processing with the consent of the data subject is one of these. Similarly, the consent of the parties involved is one of the possible exceptions to the

11. *See* Christophe Vigneau, *Information Technology and Workers' Privacy: Regulatory Techniques*, 23 COMP LAB. L. & POL'Y J. 505 (2002)

prohibition on the interception of communications set out in the federal and state laws on "wiretapping" in the United States and in the EU Directive on Privacy and Electronic Communications.[12] In this second example, because the legislation applies to all interceptions of communications (and not just to those that take part in the context of an employment relationship), employers must gain the consent not just of their employees, but also of any third parties who may be the senders or recipients of the communications. And because such consent may be difficult to get, it may prove to be a greater obstacle to an employer's plans to conduct surveillance than the requirement of gaining consent from the employees who will be the main subjects of that surveillance. (Indeed, it was for this reason that the British Government attempted to phrase its legislation on the interception of business communications in such a way as to remove the need for third party consent.)

A. The Form of the Consent

To start with consent in a contract of employment, where the law does not already require such a contract to be in written form its terms may be implied, largely from the practices accepted by both parties. Even where it is in written form, the very nature of an employment relationship means that the contract cannot set out every eventuality but only establish a general framework. Clearly then, there is a possibility that consent by the employees to surveillance and to data processing may be implied where their employer engages in such practices and they do not object. Again, there may be difficult questions—and different national answers—over the extent to which this may happen: The more intrusive a practice, the more likely the courts will not accept it as simply another, general term of employment to be implied with all the rest. To the extent to which this type of implied consent is accepted there can clearly be no formal requirements as it is given as the result of an omission rather than of an action.

Implied consent may also be taken to satisfy legislative requirements for consent (as we have seen with respect to the U.S. courts' interpretation of the "wiretapping" laws). It may be for this reason that some state-level legislation on data processing in the United States specifies a need for written authorization, which surely

12. DIRECTIVE 2002/58/EC, which will update and replace Directive 97/66/EC (the changes must be implemented into the laws of the Member States by the end of October, 2003).

implies an active acceptance that cannot be satisfied by mere acquiescence or "implied consent." German legislation goes even further in its formal requirements by stipulating that the written consent to the processing of the employee's personal data must be in an independent document. This is presumably to enhance the employee's freedom to choose whether or not to accept such processing by making it clear that the law considers the question of consent to be independent of other matters—although whether the employer in fact presents the employment contract and the consent forms in a manner which preserves this independence may be quite another question. (In any case, German law allows employers to process a great deal of personal data without the need for the employee's consent.)

In general, however, European law does not establish any specific requirements on the form that the consent must take. It is true that Directive 95/46/EC makes a distinction between "unambiguous" consent (which may be required for the processing of "ordinary" personal data) and "explicit" consent (which may be required for the processing of "sensitive" personal data). However, although this distinction was faithfully transposed into national law by the legislatures of each Member State, one does rather get the impression that nobody had the faintest idea what this distinction might actually mean in practice, and so the matter has been left for the courts to sort out. One clue as to the meaning is found in the ILO's commentary to its C*ode of Practice on the Protection of Workers' Personal Data*, where it defines "explicit" consent as meaning written consent unless there is a good reason why not; it gives the example of verbal consent being acceptable where a worker is illiterate or does not understand a particular language.

B. Consent and Free Choice

Whether consent is given in a contract of employment or in response to a legislative requirement, it is a choice that can only be exercised by the individual concerned. Only that individual can decide whether or not to agree to the conditions of a contract of employment (irrespective of whether the terms of that contract have been established unilaterally by the employer, jointly through collective bargaining, or even as a result of negotiations between employer and worker). And all the legislation which requires employee consent makes it clear that such consent must be given individually by each of the persons directly concerned: those who are

making the communications that are to be intercepted or those who are the subject of the personal data that are to be processed. Directive 95/46/EC, for example, defines "the data subject's consent," as an "indication of *his* wishes by which *the data subject* signifies *his* agreement to personal data relating to him being processed."[13]

In some Member States, this focus on the individual may give rise to tensions with the laws on worker representation. Under French and Spanish law, for example, the employees' representatives must be consulted before the installation of equipment that could be used for surveillance; and, under German law, the Works Council must consent to any installation of new equipment and to any surveillance for disciplinary reasons. All of these rights must, however, be thought of as being in addition to, and not in replacement of, the right of each individual employee to give or withhold consent. This conclusion has caused some difficulties in Italy, where the trade unions are accustomed to representing employees as a collective; sometimes they even have the power to concede certain of the employees' legal rights as part of an overall negotiated settlement with employers. The fact that individual employees now have the power to decide whether or not to give their consent may be seen as undermining this traditional role of the unions—certainly, they may have to change their function from negotiating rules for the collective to providing advice and support for the individual. Similar considerations have been expressed in terms of the function of the Works Councils in Germany.

The law in all countries must also make a policy decision about the extent to which individuals should be able to relinquish their rights as citizens when they sign a contract of employment. In countries such as the United States, where a classical, contractual interpretation of the employment relationship prevails, the scope for waiving one's own rights may be very broad indeed. As we have seen, the employer "sets the rules" and the individual's freedom consists of the decision of whether or not to accept those rules. In other countries—especially the continental Member States of the European Union—more emphasis is put on the social and economic reality of work: the law sets certain minimum standards and the parties to an employment contract cannot lawfully agree to any terms that are less favorable to the employee. The scope for consent is thus limited in order to promote wider social policies—such as the protection of workers, and the prevention of industrial conflict. In questions relating to the

13. *See* Directive 95/46/EC, *supra* note 3, at art, 2(h) (emphasis added); *see* DIRECTIVE 95/46/EC, *supra* note 3, at arts. 7(a), 8(2)(a) for similar wording.

surveillance of workers and the processing of their personal data, these national differences may be compounded by the different emphases that national legal systems may give to the protection of individual privacy. However, even in the United States, where the written agreement of the employee will usually be taken as conclusive evidence of valid consent, the law may impose limits on what the parties may agree; it has, for example, been suggested that U.S. courts might be reluctant to accept a term that allowed random strip-searches.[14] The law on contractual consent to surveillance and data processing may thus differ enormously from one country to another, albeit that in all legal systems there is probably some minimum degree of privacy that the law will preserve, no matter what the parties have purported to agree.

There is also great variation in the degree of free choice that national laws demand in the exercise of the consent required in legislation on surveillance and data processing. At one end of the scale is the "implied consent" recognized by U.S. courts with respect to the "wiretapping" legislation. Here, the choice of individuals is limited to deciding whether or not to continue with their communications once they have been notified of the possible surveillance. At the other end of the scale is the consent required for the purposes of Directive 95/46/EC, which must be "freely given, specific and informed." "Specific" and "informed" are linked to the requirement of the Directive that all data subjects be notified of the nature and purpose of the data processing. Thus, in order to give informed consent, each data subject must have been provided with all relevant information; and in order for the consent to be specific, it can only be valid for the data processing described in the notice (that is, consent to the use of data for one purpose cannot then be valid for the collection of any other data, or for any new use of the present data). Moreover, it would seem that this definition of consent implies a limit upon the purpose of the processing, which must be specific and not over-general. An interesting example here was the ruling by the Spanish Data Protection Agency that consent that purported to allow trade unions to process personal data for the purpose of "representing employees" (their Constitutionally-defined function) was too general to be acceptable. Nevertheless, there remains a considerable margin of doubt over where the boundary should be set between specific consent and general consent, and also over the closely-related question of whether consent must be given every time the employer

14. M. Higgins, *High Tech, Low Privacy*, A.B.A.J., May 1999, at 52.

conducts a particular form of surveillance or processing; or whether a general, once-and-for-all consent to a certain form of processing would be valid.

Perhaps even more significant is the requirement in the Directive that the consent be "freely given." This implies that data subjects must have a genuine option to refuse to give their consent or that, having given it, they should be free to withdraw it. This in turn may mean that employers should look for other grounds on which to justify their surveillance and data processing. The Directive sets out a number of possible circumstances in which the processing of personal data may be lawful, and consent is just one item on the list. For most forms of surveillance and data processing within an employment relationship, there will usually be alternative justifications which would allow employers to do these without having to seek consent (although they would, of course, still have to follow all of the other requirements of the Directive, which include notification). This point has been stressed by the European Union's independent committee of experts on data processing. In a report drawn up with the help of ten of the national data protection authorities, the Committee insists that consent should only be used by employers as a "fall back position," precisely because of the requirement that workers have a free choice. It argues that if a worker cannot refuse or withdraw consent without suffering some sort of prejudice—such as the loss of a job opportunity—then the consent is not genuine.[15]

C. The Legal Effect of Consent

Consent has a stronger probative value than notice as it should serve to demonstrate that the employee has received information and acted upon it. If it is given in a contract of employment, consent may authorize the employer to do whatever is envisaged by the terms in question and, if it is given in response to a legislative requirement, it may permit the employer to undertake forms of surveillance or data processing that would otherwise be forbidden by that law. However,

15. The Committee goes to great lengths to stress this opinion. They state (in bold capital letters set in a highlighted box):

> [WE TAKE] THE VIEW THAT WHERE AS A NECESSARY AND UNAVOIDABLE CONSEQUENCE OF THE EMPLOYMENT RELATIONSHIP AN EMPLOYER HAS TO PROCESS PERSONAL DATA IT IS MISLEADING IF IT SEEKS TO LEGITIMISE THIS PROCESSING THROUGH CONSENT. RELIANCE ON CONSENT SHOULD BE CONFINED TO CASES WHERE THE WORKER HAS A GENUINE FREE CHOICE AND IS SUBSEQUENTLY ABLE TO WITHDRAW THE CONSENT WITHOUT DETRIMENT.

Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, EU document number 5062/01/EN/Final, WP48 (Sept. 13, 2001).

as with notice, consent does not authorize any and all behavior by employers. As we have seen, both the legislature and the courts will probably establish certain limits as to what may be consented to in a contract of employment (albeit that these may differ enormously between countries); and the legislation which requires consent may establish other requirements in addition to that of consent. Moreover, the legal effect of consent may be further limited because of concerns over the nature and context of the consent given in a particular case: whether an employee had all the information and knowledge necessary to be able to give his or her consent and, above all, whether and to what extent there can ever be said to be genuine consent in the context of an employment relationship where the resources, information, and power of the parties tend to be very unevenly distributed.

A failure to gain valid consent may result in the employer's surveillance or data processing being unlawful and thus raise the possibility of administrative or even criminal penalties for the employer, along with the possibility of having to pay damages to the employee. Directive 95/46/EC, for example, requires all EU Member States to ensure that data controllers will be subject to legal sanctions and that data subjects who suffer damages because of unlawful processing will be able to receive compensation from the data controller. National laws may also hold that any information collected through unlawful surveillance or processing may not be admissible as evidence: so such information could not be used to support any disciplinary action taken against an employee—which may, in fact, be the very reason why the employer collected the information in the first place.

IV. CONCLUSION

Notice and consent often have an important influence on the lawfulness of surveillance at work and the processing of personal data about workers—but they are rarely the end of the story. The law may continue to offer certain protection for the privacy, autonomy, and dignity of workers, irrespective of any notice that the employer has provided and irrespective of any agreement that the parties may have made. Thus, in the often complicated task of setting a balance between the rights and interests of employers and employees, notice and consent may often be important factors to be taken into consideration, and they may have an important influence upon the outcome. But they are by no means the only factors to be considered,

which is why they usually provide us with useful and important guidance, but not with definite answers.