One of the many interesting topics of discussion at the 9th Annual Meeting of the European Institute for Computer Anti-virus Research (EICAR) this March in Brussels was privacy. In the panel discussion on privacy policies in the European Community, we touched on the issue of workplace monitoring.

A key question in any such discussion is the definition of privacy. Most experts see privacy as the result of awareness and control by the data subject. According to the stringent new rules of the European Privacy Directive, the subject should know and be able to control what information she is revealing to whom and for what purposes. This principle implies that transmission of data to authorized recipients should be confidential so that unauthorized personnel or organizations not have access to the information. In addition, once the data are collected and manipulated by an agency, the data subject must have the right to see what has been collected, to correct errors, to determine the ways in which the data may be applied or with whom they may be shared, and may remove permission for data storage and distribution.

Although there is relatively little hard evidence based on systematic, scientific investigation of attitudes and beliefs on this question, several speakers on the panel and in the audience thought that the US and Europe seem to differ in fundamental attitudes towards privacy.

* People in the US are more likely to be surprised by the European Community (EC) Privacy Directive's requirements than Europeans.

* US residents seem to take it for granted that it's acceptable to opt-in by default and opt-out explicitly from data collection; in contrast, the speakers believed, Europeans seem to start from the premise that privacy should be the baseline, with explicit opt-in required to allow data collection and sharing.

* Europeans have more faith in the privacy protections afforded by government regulations; in contrast, US residents seem to be more skeptical of all government initiatives, including privacy protection.

* In certain European countries such as Germany, employees are guaranteed baseline privacy protection with the workplace unless there are explicit civil contracts with trade unions to override these protections. For example, it is a given that an employee is entitled to privacy of a locker or of a drawer in their desk. Similarly, only if an employee willingly surrenders privacy rights would it be acceptable to monitor corporate e-mail and files on disk. In contrast, in the US, there seems to be wider acceptance of the normality of having total access to e-mail and files on corporate systems as long as the employment contract is clear on this condition.

In general, the panel and audience agreed that there are some very serious consequences of failing to make the ownership of e-mail and files clear to employees when they come on board. The worst situation arises if employees are granted the right to control personal information residing on corporate systems; under the European Privacy Directive, such employees would have the right to order the destruction of their "private" e-mail and files on disk and on backup media. The
complexity of purging backups would be enough to give any system administrator nightmares; the quagmire of deciding which files and messages are legitimately defined as corporate vs private could occasion tremendous costs and quite likely lead to litigation.

No, as I understand it -- and I am not a lawyer and this is not legal advice (for legal advice consult an attorney with expertise in intellectual property law) -- corporations should be absolutely clear when hiring staff so everyone understands that all data created by employees of an organization must be the property of that organization and that there is absolutely no right of privacy for such material.

In addition, lawyers tell me that a single signature at time of hiring is insufficient protection for the corporation. The privacy policy must be well known and seen to be enforced.

Warnings at logon may not be sufficient in Europe; I was told that some EC judges have ruled that logon banners are known to be widely dismissed by employees and therefore cannot be adduced as sufficient evidence of informed consent to full disclosure of e-mail and files on the corporate system.

My Canadian friends and colleagues warn that Canadian privacy protection is stricter than US standards and that Canada has moved quickly to conform with the EC Privacy Directive.

In summary, there seem to be different perceptions of privacy between Europe, Canada and the United States. Multi-national corporations and those doing business internationally will do well by checking their workplace monitoring policies with all the relevant legal advisors to ensure that no one inadvertently violates the strict privacy standards that are evolving in Europe today.

* * *

Mich Kabay can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.