UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 4

Fall 2000

Protecting Individual On-Line Privacy Rights: Making the Case for a Separately Dedicated, Independent Regulatory Agency, 19 J. Marshall J. Computer & Info. L. 93 (2000)

Jack Karnes

PROTECTING INDIVIDUAL ONLINE PRIVACY RIGHTS: MAKING THE CASE FOR A SEPARATELY DEDICATED, INDEPENDENT REGULATORY AGENCY

by JACK KARNS†

I. INTRODUCTION

It is difficult to identify any issue creating more legal consternation at this moment than the level to which individual online privacy rights should be protected.[1] This note evaluates both at-home and at-work considerations, with special emphasis on the latter, in reaching the conclusion that the time has arrived for creation of an independent regulatory agency that is singularly dedicated to this purpose.[2] The level of sophistication currently available in equipment and software to those who seek to violate privacy rights is so overwhelming as to render a less knowledgeable citizen helpless.[3] Our traditional common law privacy protection, particularly that which has evolved via First, Fourth, and Fourteenth Amendment case law, is simply inadequate to protect this fundamental right.[4] Finally, the Congress has not acted with the same

† Professor of Business Law, East Carolina University, Greenville, N.C. S.J.D. (Candidate) (Health Law and Policy), 2000, Loyola University Chicago; LL.M. (Taxation), 1992, Georgetown University; J.D., 1981, Tulane University; M.P.A., M.S., 1974, B.A., 1973, Syracuse University (karnsj@mail.ecu.edu).

1. Heather Green, Mike France, Marcia Stepanek, & Amy Borrus, *Privacy: It's Time For Rules*, 3673 Bus. Week 82-84 (Mar. 20, 2000) (indicating the trend in the area of privacy on the Internet).

2. *Id.* at 94.

3. Jeffrey Beard, *E-mail That Evaporates*, Natl. L.J. B11 (July 17, 2000). Some software programs can purge electronic messages after a defined period of time or days. *Id.* Several companies have attempted to improve on this model offering programs that vaporize e-mail in perpetuity in order to protect delicate and proprietary work that the employer does not want leaked. *Id.*

4. Kenneth W. Clarkson, Roger LeRoy Miller, Gaylord A. Jentz & Frank B. Cross, West's Business Law ch.9, *Cyberlaw and E-Commerce* 169 (8th ed., West 2000) Constitutional issues of online privacy show that "[t]o date, most of the Internet and new technology issues raised under the Constitution involve regulations of the freedom of speech." *Id.* Le-

proficiency in protecting online privacy rights as it has with respect to other key areas such as telephone conversations[5] and wireless communication. Both in Congress and in the courts, common law privacy rights continue to be viewed within the basic framework of First Amendment privacy rights, the Fourth Amendment warrant requirement and the exceptions thereto, and the Fourteenth Amendment. As long as this continues, online privacy rights will remain in the present, inherent state of flux that has dominated the issue since the inception of the Internet and electronic communication systems.[6]

With the evolution of privacy rights under common law concepts, it has been a difficult transition to bring within the reach of traditional legal theories modern methods of conducting business transactions and handling personal matters.[7] Employers have been quick to install sophisticated computer systems with electronic messaging and Internet capabilities.[8] Additionally, they want increased work production from employees, and yet are reluctant to sanction personal use of the aforementioned equipment even when it will enhance work efficiency.[9] Add to this the development of software that allows easy eavesdropping access to see what the employee is doing on his or her machine, and the demands of the employer create considerable friction with the employee's right of privacy.[10] Also, consider that a conversation by an employee held on the employer's telephone would be protected at a higher level by current statutory and case law while the same discussion communicated via electronic mail ("e-mail") would not, and the absolute contradiction inherent in contemporary privacy law is clear.[11]

The dilemma has reached crisis point with employers able to attach "sniffer" programs to employee machines and prohibitions against even the most minor of personal uses of employer equipment.[12] Add to this

---

gal challenges to laws that attempt to inhibit speech have generally been most successful when based on the commerce clause or the First Amendment. *Id.*

5. *Katz v. U.S.*, 389 U.S. 347 (1967).

6. David L. Hudson, Jr., *Book Review,* 86 ABA J. 86 (Aug. 2000) (reviewing *Code and other Laws of Cyberspace*). There is also concern that commercial profiteers inundate the Internet, although the Internet was developed for research. *Id.* To this observation, the author adds "privacy invaders." *Id. See also* Michael D. Goldhaber, *Cybersmear Pioneer*, Natl. L.J. A20 (July 17, 2000) (stating that defamation issues are also getting a new twist with online posters).

7. Clarkson, *supra* n.4, at 182-186.

8. Larry Armstrong, *Someone to Watch Over You*, 3689 Bus. Week 189 (July 10, 2000).

9. *Id.* at 190.

10. *Id.*

11. *Id.*

12. *But see* Michelle Conlin, *Workers, Surf at Your Own Risk*, 3685 Bus. Week 105 (June 12, 2000) (noting that workers often abuse their access to the Internet with some spending five or six hours of every work day glued to pornographic Web sites, the most

the uneven, heavy hand of some employers, dependent upon the circumstances, and the result is foregone.[13] The need for an independent, singularly focused agency has never been greater and has never had such justification.[14] This note considers privacy law, current and future, and the role it plays in the need to establish this agency. Employer misdeeds, such as those in the *Pratt & Whitney*[15] case, are discussed to bolster this position.

Finally, comments are offered to support the argument that there is no current independent regulatory agency positioned to deal exclusively with this problem, both in the home and in at-work environments.[16] The author rejects out-of-hand any efforts by the Executive Branch, such as the Department of Justice or Federal Bureau of Investigation, to play any role in this matter whatsoever. The records of these institutions speak for themselves. As for current agencies, such as the Federal Trade Commission ("FTC"), this body is charged with regulating unfair and deceptive trade, and this creates the question as to whether privacy protection falls within this agency's enabling legislation.[17] The business

---

popular type of site amongst this group of malingerers). At this rate of lost productivity, the need for sniffer software is obvious. *Id.* However, it is reported that nearly 70% of Charles Schwab's online orders come from employees' desk computers at the workplace. *Id.* at 105.

13. *Id.* at 106. The example covered here involved the issue of employee morale:

> CHANGE OF POLICY. Many companies that tried the heavy-handed approach have found that it backfired. When MediaOne Group was part of US West, Inc., the parent company would routinely send out dramatic e-mail messages threatening employees who used the Internet for personal use. Morale sank. Once MediaOne was spun off, however, executives adopted a culture that was a bit more trusting.

Id.

14. Margaret Mannix, Toni Locy, Kim Clark, Anne Kates, Joellen Perry, Frank McKoy, Hoannie Fischer, Jeff Glasser & David E. Kaplan, *The Web's Dark Side*, 129 U.S. News & World Rep. 36 (Aug. 28, 2000) (noting that misuse of this marvelous technology is not rampant, spanning the country in workplace and in the homes). Invasions of privacy have made people fear for their lives and lose faith in their hopes and dreams. *Id.*

15. *United Tech Corp. Pratt & Whitney Div. v. Turbine Kinetic, Inc.*, 1998 Conn. Super. LEXIS 562 (Feb. 24, 1998).

16. Lawrence White, *Colleges Must Protect Privacy in the Digital Age*, Chron. Of Higher Educ. B4, B4-5 (June 30, 2000) (stating that the "at-work" environment extends to include institutions of higher learning since they must also protect students' privacy rights); *see also* Florence Olsen, *Privacy Expert Advises Colleges to Bar 2 Popular Internet Tools*, Chron. Of Higher Educ. A40 (July 14, 2000).

17. *See* 15 U.S.C. §§ 41-58 (1982). Initially, the enabling legislation provided that the FTC would regulate "unfair methods of competition," but this standard was expanded in 1938 with the Wheeler-Lea Amendment to include "unfair or deceptive acts or practices in commerce." *Id.* As written, this legislation does not speak to the need to provide protection to individuals who are victimized by online privacy violations. *Id.* This problem is exacerbated by the FTC's general remedy limitation of issuing cease and desist orders to the offending company with remedial and corrective actions extremely limited. *Id.*

community, in general, supports the delegation of work related privacy issues to the FTC given its well established involvement in business regulation.[18] But is this position self serving, and would it really protect the worker adequately?[19] The friction between employer and employee in this area is clear and not to be taken lightly. An employer must be concerned about improper use of Internet assets, for example, to access sexually explicit sites that might lead to "hostile work environment" charges.[20] Equally important are the concerns of the employee who used the electronic messaging system to promote a pro-union position relative to distribution of information regarding an upcoming National Labor Relations Board ("NLRB") sanctioned election, as was the situation in the *Pratt & Whitney* case.[21] Accordingly, the author concludes that the FTC is not well situated to take on this aspect of the regulatory task and that a comparable consumer and worker oriented agency with separate and distinct enabling legislation is needed to protect fundamental constitutional rights in this area.[22]

---

18. Green, France, Stepanek & Borrus, *supra* n. 1, at 94 (noting that the position set forth by the staff writers at *Business Week* is typical). The writers' position is as follows:

> We favor giving the job to the Federal Trade Commission, which has begun moving aggressively on the issue of Internet privacy and which already enforces the Children's Online Privacy Protection Act, the Truth in Lending Act, and the Fair Credit Reporting Act. The agency should be empowered to impose stiff penalties for violations.

Id.

Just as the writers make their case for the FTC, they continue with a litany of futuristic developments that render the recommendation meaningless as the FTC could not possibly administer the following:

> PRIVATE PROTECTION. Of course, any privacy laws will need to evolve. As the Internet makes its way onto cell phones, watches, and other devices, some of the privacy rules that make sense in a world of desk bound PCs may become irrelevant. And the long-term prospect of biometric authentication – where fingerprints and retinal scans may be used as New Age passwords to Web sites – will certainly raise serious new privacy issues. Such a scheme will require nothing less than a national database of identifying biological data, raising the specter of abuse by both outlaw hackers and Big Brother prosecutors.

Id.

This hardly makes the case for turning the privacy issue over to the FTC as opposed to creating a separate independent agency dedicated to the sole purpose of protecting privacy rights.

19. *Id.*

20. Armstrong, *supra* n. 8, at 190.

21. Kenneth R. Dolin & Rozmus, *Regulating Employee E-mail*, Natl. L.J. B5 (July 31, 2000).

22. *See* Amy Borrus, *Web Privacy: That's One Small Step*, 3690 Bus. Week 50 (July 17, 2000) (stating that although the FTC is supported by the industry as the best bet for overseeing online privacy issues, the FTC recently came under fire for agreeing to a set of guidelines that had been developed by Internet merchants). How can the FTC be the agency of choice if it cannot take the required time to research and develop such guidelines? *Id.* Further, privacy protection is far removed from the purposes for which the

II. CURRENT EMPLOYER ENFORCEMENT

The case of *Pratt & Whitney* is very instructive relative to the at-work impact an employer can have on privacy rights. In this case, the employer had a written policy prohibiting employees from utilizing company facilities for non-business e-mail transmissions. This rule was not strictly enforced, and more importantly, about 80% of the firm's business was conducted with employees communicating with each other or with management via e-mail.[23] When a union organization drive began, Pratt & Whitney decided to tighten up on the enforcement of the workplace communication rule, and monitored transmissions so it could take punitive action against employees who transmitted pro-union messages.[24] The issue was quickly taken to the NLRB where its Division of Advice rendered a legal opinion that Pratt & Whitney actions were unlawful.[25]

The Division considered two basic questions. First, it looked at whether or not the employer's computer network was a work area such that the transmission rules could be selectively imposed, and, secondly, it questioned whether or not the dissemination of an e-mail message was in fact a distribution of that message or rather a solicitation regarding union activity.[26] These are important privacy questions for the employee and the answers that the Division gave are instructive relative to determining the current state of privacy laws that exist today. As to the first question, the Division of Advice agreed that the employees operated within a work area relative to the time that they were supposed to be there and the computer equipment that they used to complete their work. This meant that the computers were "inextricably intertwined" with the employees' need to occupy the space and to complete the work that was assigned by the employer.[27] At this point, the analysis or resolution of the second issue was essentially very relevant because the NLRB has strict rules governing any employer restrictions prohibiting

---

agency was established in 1915. *Id. See also*, Robert L. Hoegle and Christopher P. Boam, *Putting a Premium on Privacy Protection Polices*, Natl. L.J. C8, C8-C11 (Aug. 2000); Laura Neuwirth, *Regulating OnLine Goods*, Natl. L.J. C1, C18-19 (Aug.2000) (discussing the Consumer Product Safety Commission's developing interest in monitoring Internet sales); Mark W. Merritt, *Web Puts New Spin On Traditional Antitrust Laws*, Natl. L.J. C5, C5-C8 (Aug. 21, 2000) (noting that the FTC also governs certain antitrust activities that are deemed anticompetitive and that the Internet is having a profound effect on this issue as well). Add this matter to the existing list of regulatory responsibilities of the FTC, and whether it can effectively monitor privacy issues becomes even more suspect. *Id.*

23. Dolin & Rozmus, *supra* n. 21, at B5.

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.*

solicitation or distribution of pro-union organization materials.[28]

According to the NLRB's rules, an employer may ban distribution of pro-union materials during work hours and in work areas; however, the prohibition of union solicitation activities only applies to the time the employee is on the company clock. This means that if the electronic messages were deemed distributions, the employees would have an argument that the application of the rule was effectively over broad.[29] This would lead to the argument that they should have the opportunity, within reason, to transmit pro-union messages, especially on personal time.[30] The Division determined that the transmittal of e-mail by Pratt & Whitney employees was solicitation.[31] Since the transmittal of the e-mail could be viewed as someone having received a brochure in a traditional union organizing effort, he or she would be permitted to respond in a reasonable fashion. As a result, the Division concluded that at least a portion of the employees' e-mail transmissions deserved protection as union solicitation that could have occurred on free time. The employer's total ban against using company equipment was effectively unlawful.[32] The ban applied to all messages regardless of whether they were communicated during work hours or non-working time, and this was over broad in the strictest sense.[33]

To bring this issue into a setting that might have occurred a decade ago, it should be compared to an employee walking by a company bulletin board on the way to another work area and taking a couple of seconds to post a brochure on the board soliciting union support. There is no way that the NLRB would view this as inappropriate solicitation activity on the part of the employee. Similarly, if the employer were to come by and rip the brochure off the board because it had been placed there "during work hours" the NLRB would likely rule that the employer had violated the National Labor Relations Act.[34]

There is no question that the simple analogy put forth in the previous paragraph is certainly inadequate to fully compare the factual situations of pre e-mail unionization efforts with those that are occurring in the work place today. However, *Pratt & Whitney* certainly marks a very important development with regard to demonstrating the limits placed on an employer in restricting the privacy communication rights of indi-

28. *Id.*

29. Dolin & Rozmus, *supra* n. 23, at B5.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *National Labor Relations Act*, 29 U.S.C. § 7 (1994) (providing that "employees shall have the right to . . . engage in other concerted activities for the purpose of collective bargaining or other mutual aid and protection.").

vidual employees. In fact, it might even be concluded from *Pratt & Whitney* that if electronic messaging is used at a proper time in soliciting pro-union support, the employer has less ability to control or restrict the transmittal of these messages than if it was being done with traditional paper brochures and fliers.[35]

From the *Pratt & Whitney* case, some basic rules can be discerned relative to the development of any privacy policy regarding the personal use of an e-mail messaging system. An employer should consider the breath and scope of the enforcement practice whether or not the rule is enforced at all.[36] The employees alleged misconduct should always be delineated as having occurred during work hours as opposed to non-work hours.[37] Also, the issue of how much time the employee spends working on the computer to complete company business and whether the alleged misconduct interfered in the completion of this work should be considered.[38] Finally, the language of any privacy rule regarding e-mail messaging must be precise relative to the type of communication that it prohibits, and should clearly state who is prohibited from participating in that communication.[39] These guidelines are offered so that an employee can carefully review an employer's privacy policy intelligently and be able to determine whether he or she is being fairly treated.

III. THE FTC'S ROLE IN TRADE PRIVACY PROTECTION

Previously it was stated that the FTC would not be the proper independent regulatory agency to protect an individual's privacy rights relative to use of electronic messaging in the work place.[40] Statements regarding the FTC's role in protecting consumer privacy must be conditioned with a caveat that the agency plays an extremely critical role relative to the monitoring of companies that market their products on the Internet and which collect consumer information either through independent surveys or through actual purchase transactions. To enhance

35. Dolin & Rozmus, *supra* n. 23, at B5.

36. *See* Robert A. Stein, *Join Us on the Web*, 86 ABA J. 93 (Aug. 2000).

37. Diane E. Levine, *At-Work Privacy*, PC Privacy, Smart Computing Guide Series, vol. 8, issue 4, 66.

38. Paul Sloan & Marcia Yablon, *New Ways to Goof Off at Work,* 129 U.S. News & World Rep. 42 (Sept. 4, 2000).

39. Diane E. Levine, *Personal-Information Privacy*, PC Privacy, Smart Computing Guide Series, vol. 8, issue 4, 60.

40. This opinion is primarily based on total agency caseload and responsibility rather than on whether the FTC would be a fitting venue for monitoring this crucial issue. The FTC has distinguished itself as being one of the most active, bipartisan regulatory bodies in Washington. There is no need to assign it a task that would almost certainly burden it with assignments that it could not possibly achieve without a significant re-tooling at the lowest of levels. This might also have the adverse impact of derailing the FTC's well established record in unfair and deceptive trade practice regulation.

its role in this area the agency often declares Internet Web site surf days where all staff members go from one Internet site to another checking the privacy declaration on the home page.[41] There is no question that when it comes to evaluating the Internet super highway, that information is the key to success of any emerging business within that particular marketplace. Whether a company is going to succeed or not depends upon its ability to gather and use information about the customer base to which it wants and needs to market products. Obviously, the efficiency and the quickness with which the consumer information can be accumulated and used is also a factor.[42]

But privacy problems arise with respect to how the consumer information is collected either by the company that intends to sell the products or some other clearinghouse firm that offers consumer lists and other relevant consumer information for sale. The question here is what the FTC's role should be in limiting and regulating access to consumer information as well as giving the consumer the opportunity to limit a company's right to collect information that will be used by a company operating on the Internet.[43] Before this issue is discussed further, the primary thrust of this note has been issues of personal privacy as defined in the common law and used to protect individual rights at home and in the workplace. The protection of the individual consumer from unfair and deceptive collection of personal privacy data on the Internet is just as important a privacy matter as those issues raised previously regarding electronic messaging.[44]

The FTC became particularly concerned about the collection of consumer data when the New York based DoubleClick company merged with a mail order company called Abacus and stated that it planned to

41. Hoegle & Boam, *supra* n. 22, at C8-C11 (summarizing the current role of FTC and how the agency has brought the issue of online privacy within the its area of responsibility). Straying from the constraints of a developed privacy policy can have legal ramifications. *Id.* The FTC stated in 1998 that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act. *Id.* For example, an investigation by the FTC led to an administrative proceeding against GeoCites (and ultimately a consent decree) because GeoCites allowed the third-party collection and use of personally identifiable information on Web site users, contrary to the company's own privacy policy. *Id.* Since the GeoCites consent decree, the FTC has engaged in periodic review of Internet content under the aegis of the agency's antitrust enforcement and consumer protection jurisdiction. *Id.*

42. *Id.* (stating that this function would still not adequately allow the FTC to fulfill the primary role of regulator and protector of individual privacy rights). The FTC's Internet Task Force engages in Internet surf days, when task force members review the advertising and privacy claims made by certain sites. *Id.* Frequently, FTC staff will e-mail a site administrator, notifying the site of a violation and giving the site 30 days to comply with requested changes. *Id.*

43. Green, France, Stepanek & Borrus, *supra* n. 1, at 50.

44. Hoegle & Boam, *supra* n. 22, at C8-C11.

combine names, addresses, and personal data for sale to Internet company users.[45] This database would consist of tens of millions of customers in the company's online profiling system and caused considerable uproar among privacy experts.[46] DoubleClick attempted to argue that its focus was on anonymous products and that it had no plans to link names with personal identifiable information, but skeptics remained unconvinced.[47] In order to assuage the complaints concerning the DoubleClick-Abacus merger, the Network Advertising Initiative ("NAI"), which is a consortium of companies representing 90% of the Internet advertising industry, promulgated a set of privacy rules for its members.[48]

The privacy rules, accepted by the FTC, have been criticized as being too pro-industry.[49] In a nutshell, the NAI standards allow consumers to opt out of any collection of anonymous data on the Internet or be offered an opportunity to have previous collected data removed from the system entirely.[50] The FTC voted four-to-one in accepting these voluntary standards with the lone dissenter being FTC Commissioner Orson Swindle.[51] Mr. Swindle argued that privacy legislation as offered by the NAI was insufficient and that the FTC should continue to press Congress for legislation that would require commercial Web sites to inform all visitors about what information is or is not being collected about them and how it will be used.[52] Regardless of whether Congress decides to promulgate a privacy law to displace the NAI consumer rules, the author supports a limited supplemental role for the FTC in this privacy protection area.[53] It is with respect to privacy rights as an individual in the work place, in the home, as a citizen in personal activities such as seeing a physician or going to a hospital, or as a citizen exercising constitutionally protected rights, that the author supports the establishment of an independent

45. D. Ian Hopper, *Online Privacy Rules OK'd*, News & Observer A1, A15 (July 28, 2000).

46. *Id.*

47. *Id.*

48. Federal Trade Commission, *FTC Issues Report on OnLine Profiling*, ¶ 2 <http://www.ftc.gov/opa/2000/07/onlineprofiling.htm> (accessed Nov. 17, 2000.); *see also*, Electronic Privacy Information Center, *Network Advertising Initiative: Principles not Privacy* <http://epic.org/privacy/Internet/NALanalysis_.html> (accessed Nov. 17, 2000).

49. Hopper, *supra* n. 45 at A1, 15A. The Electronic Privacy Information Center in Washington, D.C. has announced its intention to initiate legal action against the FTC to force adoption of stronger measures. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. Where product promotion crosses both the lines of deception and the personal privacy of the consumer, the FTC should be permitted to issue a cease and desist order to handle all aspects of the problem. The difficulty with mandating that the FTC regulate all online privacy violations is its existing workload, as well as its restrictions in formulating remedies.

regulatory agency.[54]

IV. CONTEMPORARY DEFINITION OF PRIVACY

The common law principle of invasion of privacy envisions an unreasonable intrusion into an individual's space. Commentators have referred to this principle as an "inalienable right" or "the right to be let alone.[55] With the development of electronic means of communication, a key issue has been that of consent.[56] For example, if the employer tells, or warns, the employee that the work place is subject to a certain level of surveillance, does the employee consent by virtue of signing the employment contract?[57] Comparable to this approach is the required signing of a release by the employee in conjunction with the employment contract acknowledging said surveillance, or the warning at the beginning of a telephone call that the conversation may be monitored or recorded to ensure accuracy, for training purposes, or to ensure consumer protection.[58] The argument put forth by the employer is that privacy rights are forfeited in all instances.[59] This implied consent doctrine has been utilized by courts to uphold such employer action even in the light of a changing work place and work force.

Previously, all work was completed at a central location with all employees coming together and using company owned equipment to accomplish assigned tasks. In this environment, the employer had considerable authority to monitor the usage of its equipment, not to mention the activities of all employees.[60] Also, the workday was more easily broken into employer time and employee time, starting time and quitting time, lunch time, and break time.[61] Clearly, the importance of these de-

54. *See* Lori J. Braender & Kara McCarthy Perry, *Making a Virtual House Call*, Natl. L.J. C1, 16-17 (Aug. 21, 2000) (reporting that the New Jersey task force on telemedicine recommended special legislation to address licensure, privacy, quality of care and technology in regards to the unique nature of technology used in medical practice).

55. Amitai Etzioni, *The Limits of Privacy* 190 (Basic Books, 1999) (quoting Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890), and U.S. Office of Science and Technology, Privacy and Behavioral Research, 3 (U.S. Government Printing Office 1967)).

56. *Id.* at 155-60 (examining the issue of informed consent in the medical file context).

57. Lori Robinson, *Surfing Incognito*, PC Privacy, 8 Smart Computing Guide Series 4, at 91 (explaining that an employee can take defensive action by encrypting messages or covering online trails); *see also,* Monique I. Cuvelier, *Sending Anonymous E-mail*, PC Privacy, 8 Smart Computing Guide Series 4, at 93.

58. Tom Nelson and Mary O'Connor, *The Browser Trail: How to Delete Your Tracks,* 8 PC Privacy, Smart Computing Guide Series 4, at 99.

59. Etzioni, *supra* n. 55, at 155-90.

60. *Cf.* Levine, *supra* n. 37, at 66, 68 (explaining that although employees generally feel that electronic monitoring is an invasion of privacy, most employers feel justified [and are justified] in monitoring or spying on their employees).

61. *Id.* at 67.

lineations is that the rights of employees, vis á vis the employer's right to monitor, could be segmented much more easily than is the case today. Even where an employee might use an employer's computer to send personal e-mail, the employer's right to monitor could be more easily defined.[62] This is due to the fact that the courts recognized with some limited degree that even employer equipment could be used for personal purposes with the key factor being whether the individual was doing so on "company time."

Today the workplace environment has changed dramatically.[63] Workers no longer congregate at a central location, they are much more apt to work, at least in part, at home or on the road. Some traveling representatives spend more time in their car, in client's offices and at home than at any central location. For some of these employees, there is no central location even if a desire existed to establish a presence there.[64] Not only is this in accordance with the changing face of the work place, it is in accordance with efforts to minimize the investment of firms in brick and mortar capital structures or rental payments for such structures when they are not needed.[65]

This issue is compounded when it is revealed that an employee may use his or her own equipment to accomplish some or all of the employer assigned tasks.[66] What are the surveillance rights of the employer in that particular situation? Certainly, they are diminished relative to the case of workers congregating in a single location and relying exclusively on employer-owned property. Issues that are even more difficult arise when an employee uses personal equipment to hook up to a company network that allows for a more complete dissemination of the individual's work and greatly enhances his or her ability to work on the run.[67] Scenes of traveling employees in airport terminals with lap top computers plugged into telephone modems are becoming the norm, not the exception. Hotels advertise that rooms have modem work stations, while airline frequent flier clubs boast access to similar facilities for the harried business traveler trying to accomplish as much work as possible between flight connections. The workday is being torn apart such that it is but a mere image of its former self.[68] Workers can arise at late night hours and complete work that in previous years would have required a trip to the office. Accordingly, the question remains the same: if the employee is using personal equipment or working to complete assigned

62. *Id.* at 66-67.
63. *Id.*
64. *Id.* at 67.
65. *Id.*
66. Levine, *supra* n. 37, at 66-67.
67. *Id.*
68. *Id.*

tasks at an hour that typically falls outside the prescribed workday, what are the employer's surveillance rights?[69] The answer to this question is not an easy one.

The e-mail intrusion issue is perhaps the most invasive.[70] In a nutshell, the best legal advice is do not put anything into an electronic message that you would not be willing to see printed as the headline in the Washington Post tomorrow. Employers are well aware of their rights in this area and have pushed the envelope in gathering personal data on individuals that never would have come to light without the showing of probable cause and the issuance of a warrant.[71] Proponents point to the role of the FTC and its success in this area. However, the consuming public must be made excruciatingly aware that the FTC deals only with the misuse of consumer data once it has been improperly collected by a company, not generally the employing company.[72]

Internet banner advertising is designed to insure that "cookies" are attached to even the most innocuous of responses so that as much data as possible can be gathered about the prospective client, and the FTC is responsible for guarding against "unfair and deceptive" trade practices in this area.[73] Further, there is no question that the selling of these "cold call" lists has generated unsolicited commercial e-mail, or "spam" mail, for everything from products to credit cards with pre-approved limits.[74] The receiving companies run the names through various credit and law enforcement checks and quickly cull those that are deserving of the personal attention of a letter or telephone contact. It is the regulation of this activity that most businesses would readily turn over to the

---

69. *Id.* at 66-68.

70. Jennifer Farwell, *Where Everybody Knows Your Name: Marketers Combine Offline Databases with Online Profiling to Target You*, 8 PC Privacy, Smart Computing Guide Series 4, at 28.

71. *Avoiding Commercial Internet Legislation: Corporations Push Big Brother to the Fringes of Cyberspace*, 8 PC Privacy, Smart Computing Guide Series 4, at 129.

72. To demonstrate the wide-ranging impact of the privacy issue, the following articles articulate collateral matters that do not often come to mind when evaluating the FTC's ability to takeover this area of regulation. *See e.g.*, Janet McDavid & Corey Roush, *Antitrust — Electronic Media*, Natl. L.J. B7 (July 17, 2000.); Jane Kaufman Winn & James R. Wrathall, *Bankruptcy Law — Internet Customer Databases* Natl. L.J. B8 (Sept. 18, 2000); Andrew J. Frackman & Robert M. Stern, *Patent Law — E-Commerce Damages Awards*, Natl. L.J. B10 (July 3, 2000); Bruce G. Joseph & Scott E. Bain, *Copyright Law — DMCA Safe Harbor Provisions*, Natl. L.J. B8 (July 31, 2000); Scott Winkelman & Dylana Blum, *E-Commerce — Electronic Signatures Act*, Natl. L.J. B10 (July 17, 2000); Michael Starr & Jordan Lippner, *Employment Law — Investigating Misconduct,* Natl. L.J. B7 (Aug. 21, 2000)

73. *See* David Kleinbard *Web has its Eye on You; Advertisers and marketers stalk Web users behind the scenes.* <http://cnnfn.com/2000/03/06/technology/privacy_main> (Mar. 6, 2000) (discussing and defining "cookies").

74. Farwell, *supra* n. 70, at 28-30.

FTC rather than a separate agency,[75] but they would also include the general privacy protections of individuals whether in a consumer, patient, or worker context.[76] Although the author is somewhat persuaded that the FTC could handle the purely cease and desist aspect of the problems created by certain advertising falling within its purview, a more important question is whether to categorize all online privacy problems as falling under the same umbrella, be they consumer or worker related.[77] The primary reason for this is that court cases and congressional statutes have a definite pro-business prejudice overlooking the key constitutional rights of individual consumers and employees.[78]

The foregoing raised perhaps the most important of the privacy issues from an individual perspective. Does an individual or a worker have more to fear from improper surveillance of the electronic environment by the United States government or domestic multi-national corporations seeking to gain additional market share?[79] Many claim the latter as opposed to the former, although there is plenty of finger pointing to go around. The United States government's role in privacy surveillance is affiliated essentially with the protection of information of a classified nature so as to ensure that it does not fall into the hands of foreign countries or their citizens.[80] Agencies such as the National Security Agency, Central Intelligence Agency and the Defense Intelligence Agency headline a small list of agencies that have, on occasion, overstepped their bounds in the zealous attempt to protect national classified data.[81] To the credit of these agencies, they have also thwarted numerous attempts at pilfering proprietary data, both within the public and the private sectors, that if compromised would produce serious injury to the defense of this country or to private business.[82]

---

75. *Cf.* Heather Green et al., *supra* n. 1, at 83-96.

76. *Id.*

77. 15 U.S.C. § 45(b) (1982). By statute, the FTC is limited to imposing a cease and desist order as a remedy. *Id.*

78. *See also* Associated Press, *Online Privacy Rules OK'd*, The News and Observer, 1A, 15A (July 28, 2000).

79. Associated Press, *Congress Probes FBI E-mail Snooping Device*, Daily Reflector, A4 (July 27, 2000) (explaining that congressional lawmakers of both parties questioned members of the FBI regarding the use of a software programs called "Carnivore" in criminal investigations).

80. Jack E. Karns, Roger P. McIntyre and Ernest B. Uhr, *Corporate Espionage in the Global Market: The Federal Government's Role in the Protection of Private Sector Trade Secrets*, 25 Ohio N.U. L. Rev. 331 (1999); *see also*, Ross L. Crown, *Plugging Leaks in Federal Contracts*, Natl. L.J. B17-18 (July 31, 2000).

81. Heidi V. Anderson, *The Concealment of Echelon: A Network of Spies in a Web of Lies*, 8 PC Privacy, Smart Computing Guide Series 4, at 72.

82. *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998) (explaining the policy behind the Economic Espionage Act of 1996).

These agencies have been particularly helpful to the private sector with the passage of the espionage act in 1996 that allows them to work closely with private sector companies to protect proprietary data.[83] Consequently, it is important to recognize the threat posed to the United States by foreign states and their agents, and the need to acquiesce in a certain amount of electronic surveillance needed to curb these activities.[84] As a result, any criticism levied against governmental agencies that spy on electronic communications must be tempered with this acknowledgment. Again, the author believes that the best way to protect individual consumers and workers in this national security debate is to have their rights zealously protected by an agency that does not have to cull between those cases that involve classified data and those that do not. Only a separate, regulatory agency can accomplish this function.

V. CONCLUSION

What course should be followed with regard to the evolution and development of online privacy law must be considered with several key factors in mind. First, as discussed above, the whole dynamic of the work place has changed thereby bringing into play the question as to whether any concomitant change in privacy law is needed at all to deal with this change. The common law has been molded to fit many changing areas, and although a particular positive of our legal system is its inherent nature as "living law," the question arises here as to whether specific alterations are needed to correct what could be significantly misguided deviations from the nature and purpose of the Constitution.[85]

This note has attempted to make the case that regulatory action would be an acceptable manner to deal with a societal and cultural change that appears to be more complex than existing law can manage. An analysis of the need for any change to the existing law is always a critical necessity prior to espousing the view that, in this case, a separate regulatory agency should be established to monitor consumer and employee online privacy rights. The foregoing has demonstrated that, al-

83. 18 U.S.C. § 1831 (2000). Prior to enactment of the EEA, the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1801 (1994), provided some assistance in guarding the privacy of private citizens and in protecting proprietary trade secrets; *see also*, Karns, supra n. 80, at 331 (explaining that FISA was really directed at espionage that threatened the United States).

84. Karns, *supra* n. 80, at 332 (providing that the intelligence community within the United States is a complex mix of agencies and bureaus, independent and executive, military and civilian that combine to provide protection to espionage and terrorist threats).

85. Clarkson, *supra* n. 4, at 169 (noting that the issues are unique due to the Internet's ability to cross political and geographic borders, coupled with the inability of current technology to effectively filter out what legislators and government regulators might want to filter).

though there may be no need for statutory intervention, there is demonstrable need for separating this developing issue from that which existed in the past.[86] It remains an unanswered question whether the desired goal will be achieved with the establishment of such an agency.[87]

Common law courts have traditionally looked to whether any change promulgated by a case is the least intrusive means available to effect the desired or needed change. Certainly, the passage of enabling legislation for an independent agency to regulate and protect online privacy would be much easier to accomplish than the passage of sweeping privacy legislation.[88] Should the latter be accomplished, the question would remain as to what agency, if any, would be responsible for its enforcement.[89]

---

86. *"P" — Word Paranoia*, U.S. News & World Report 16 (July 24, 2000) observes:

> As is so often the case, as a nation, we seem to be moving in two very different directions at once. There is no shortage of TV wannabes beating down the doors to battle it out with other would-be 'survivors' on a desert island, marry a total stranger on national television, or embarrass themselves silly auditioning before live cameras for a noisy boy band. But many more worry about the incessant, incremental invasions on their privacy. Telemarketing calls during the dinner hour, personal credit records that fly off, seemingly, to all points of the compass; incursions like those have prompted a growing sense of unease among many Americans. Sure, reality TV is a certifiable phenomenon, skewing ratings and driving advertiser dollars in ways previously unimagined. But of far greater moment to most Americans is what's happening to their personal zones of privacy. How to ensure the confidentiality of our medical and financial records? How to keep our kids' Internet chats and E-mails away from prying eyes? In age of exploding technological innovation, everything, it seems, is possible; including the novel but nearly paralyzing crime of 'identity theft.'

Id.

87. Borrus, *supra* n. 22, at 50. The FTC's ready acceptance of industry-generated guidelines for regulating Web advertising does not square with the agency's own call for federal legislation, a call made in May 2000. *Id.* At least a separated, dedicated agency would not have conflicting missions as presented through its enabling legislation. *Id.*

88. *Id.* Although the FTC has called for federal legislation, the industry recognizes the ease in simply assigning the role of privacy police to the FTC. *Id.*

89. Clarkson, *supra* n. 4, at 169. The United States is far from being alone in this quandary. "China and some European countries, among other nations, have attempted, with varying success, to block what their governments believe is bad for their citizens." *Id.* While the United States decides privacy issues on a case-by-case basis, Australia and Canada have active privacy legislation in place. *Id.*; *see also*, James D. Taylor & Terri J. Seligman, *International Law: E.U. Privacy Directive*, Natl. L.J. B10 (Aug. 14, 2000). Hong Kong has been overwhelmingly unconcerned as to its citizens' privacy rights while the European Union approved a privacy directive in October 1995. *Id.* South Africa's approach more closely mirrors that of the United States in that the Open Democracy Bill defines citizens' rights to government information, much like our Freedom of Information Act and various state and federal sunshine acts. *Id.* Interestingly, Russian personal privacy is protected by a statute known as the law of the Russian Federation on Information, and Information Protection passed in 1995. *Id.* The statute defines individual privacy, how individual data may be used as well as placing restrictions on information technologies. *Id.* Most importantly, the Russian Duma is working to insure that the law is applied with equal force in private and public environments, and that it be updated to comply with the European Union ("EU") directive. *Id.* This latter directive provides privacy guidelines for

Otherwise, we would look to the Executive Branch for enforcement, and as stated earlier, this is unacceptable for a variety of reasons.[90] Executive Branch enforcement is too closely aligned with political goals and agendas, whereas an independent agency owes its allegiance to Congress, with the commissioners or board members having been appointed by the President. This is an acceptable compromise in terms of trying to de-politicize an area of law that is most assuredly going to become even more difficult to administer as the way we work and live our private lives becomes more indistinguishable relative to the protection of privacy rights.[91]

---

member states and went into effect in October 1995. *Id. See also* Jeff Dodd, *Us vs. Them: How U.S. Privacy Concerns Compare With Rest of World*, 8 PC Privacy, Smart Computing Guide Series 4, 10-12 (showing that presently, at least two-thirds of the member states have approved the guidelines with the EU, making clear that it would resort to litigation if necessary in order to achieve compliance).

90. *See* Associated Press, *Internet Becoming Critical Aspect of Divorce Proceedings*, The Daily Reflector B2 (July 25, 2000). The Internet is increasingly being used to facilitate aspects of litigation investigation in areas that heretofore were never considered as likely targets. *Id.* One such area is that of divorce as private investigators realize that the Internet and electronic messaging records include a wealth of material that can often sway a case to one party or the other. *Id.* This is particularly true in states like North Carolina that still recognize fault, such as adultery, as a basis for divorce. *Id.* In this type of case, proving fault would provide the complaining spouse with a heavy arsenal to establish custody rights, rights to additional property, along with a host of other matters. *Id.* Even divorce attorneys and the American Bar Association's Family Law Section are not certain as to the privacy that should govern the use of this new discovery tool. *Id.* Certainly, standard rules of civil procedure were written long before this type of evidence was available or could even be generated. *Id.*

91. Clarkson, *supra* n. 22, at 169, sums up the problem as follows:

> One of the basic questions involved in this issue concerns how much freedom of speech we are willing to sacrifice to allow the government to further a particular value, such as shield children from certain material or preventing terrorism and crime. Phrased another way, how much of any value are we willing to sacrifice to protect our freedom of speech? There is no clear, definite answer to this question. Generally, the courts hold that speech may be restricted to serve a 'compelling interest' but only if the restriction is the 'least restrictive means' of doing so.

Id.