Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 19 *Volume XIX*
Number 3 *Volume XIX Book 3*

Article 4

2009

Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe.

Matthew A. Chivvis
Morrison & Foerster LLP

Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe.

Cover Page Footnote
I would like to thank the Honorable Judge James Ware and Professor Susan Freiwald for their insights and inspiration.

Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe

Matthew A. Chivvis*

> "[N]umerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1]

* Associate, Morrison & Foerster LLP; B.S., University of Wyoming; J.D., *magna cum laude*, University of San Francisco. I would like to thank the Honorable Judge James Ware and Professor Susan Freiwald for their insights and inspiration. This Article represents the views of the author, and should not be taken to represent the views of any other person or entity.

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

INTRODUCTION

In 1890, the Harvard Law Review published Samuel Warren and Louis Brandeis's article, *The Right to Privacy*,[2] changing forever the face of privacy law.[3] Arguably, Warren and Brandeis attempted to import an idea of privacy more at home in Europe than here in the United States,[4] for they sought to establish a means by which people could protect their own dignity;[5] however, they only tenuously founded that means on aspects of personal liberty.[6] Thus, the approach the two path-breaking authors took may represent an anomaly in the law of this country.[7] While various

---

2 *Id.*

3 *Cf.* ALPHEUS MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946); Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (describing Warren and Brandeis's article as the "most influential law review article of all").

4 *See* James Q. Whitman, *The Two Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1204 (2004) ("Warren and Brandeis undertook the seminal, and still most cited, effort to introduce a [European]-style right of privacy into American law.").

5 *See* Warren & Brandeis, *supra* note 1, at 214–15 ("The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position and station, from having matters which they may properly prefer to keep private, made public against their will."). Warren and Brandeis also equated the right to privacy to "the more general right to the immunity of the person,—the right to one's personality." *Id.* at 207.

6 Noticeably, Warren and Brandeis, while drawing many analogies to other areas of law such as intellectual property, did not directly implicate constitutional liberty concerns, such as the Fourth Amendment, or a notion of "freedom." *See id.* at 207. While they did note early in their article that the rights to liberty and property have expanded as society has developed, they did so to illustrate how "the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without interposition of the legislature." *Id.* at 195.

7 *Compare* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (suggesting that privacy is not an independent value at all but rather a composite of interests), *with*

forms of the tort protecting against invasion of privacy exist today under state common law, shortly after the time Warren and Brandeis made their argument for the tort, the focus of privacy law in this country returned to a foundation more uniquely American—one based on liberty.[8]

Why does each side of the Atlantic concentrate on a different aspect of personhood, liberty versus dignity, as the core inviolable right warranting privacy protection? Perhaps the United States favors values of liberty, especially liberty against the government, due to its founding influences. That may explain why the American right to privacy, at its core, means freedom from intrusions of the state, especially in one's own home.[9] Similarly, maybe European favor for values of dignity stems from an Old World ethos, concerned with the importance of not losing public face. After all, Europeans consider privacy to be the right to protect one's personal reputation from attack and one's personal information from exposure or mishandling.[10]

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 964 (1964) (analyzing privacy tort law in light of Warren and Brandeis to show how Prosser was mistaken).

[8] In his dissent in *Olmstead v. United States*, which found a government wiretap to be constitutional, Brandeis quoted an earlier decision of the Supreme Court. Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting). He explained, "'The principles laid down in this opinion affect the very essence of constitutional liberty and security[,]'" and "'[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense,'" rather "'it is the invasion of his indefeasible right of personal security, personal liberty and private property.'" *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). Brandeis went further to note, "Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.* at 473. While Brandeis occupied the minority in *Olmstead*, the Court ultimately accepted his view, at least to some extent, in *Katz v. United States*. *See* 389 U.S. 347 (1967).

[9] *See Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616, 630 (addressing the "sanctity" of the home); *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 5 (2000).

[10] *See* Whitman, *supra* note 4, at 1161 (describing the core European privacy rights as the "rights to one's image, name, and reputation, and what the Germans call the right to information self-determination—the right to control the sorts of information disclosed about oneself" (emphasis omitted)).

Whether the foundation of the liberty versus dignity distinction came about for the reasons above, or for other reasons, matters little for purposes of this Article. What really matters is the legal effect of the distinction. While, on both sides of the Atlantic, the differences in privacy policies influence many areas of law, this Article focuses on but one of those areas: privacy in the workplace. Currently, workers in the United States face the risk that their employers will monitor them, not only as to their activities in the ordinary course of business, but also as to their personal electronic communications made from work.[11] To be sure, the potential for real monetary and legal liabilities often forms a valid cause for concern, which motivates employers to monitor their employees, but that does not mean that the employees should be completely without protections. Yet, the current laws do little to protect employees from unwanted and unnecessary surveillance by their employers.

To remedy this problem, Congress should increase the level of protection it provides to employees by supplementing the liberty considerations of American privacy law with some of the dignity protections found in Europe. Specifically, Congress should modify the Electronic Communications Privacy Act ("ECPA") by amending the consent provision of 18 U.S.C. § 2511(2)(d)[12] and adding a similar consent provision to § 2701(c).[13] In each case, the amendment should require express written consent of the person subject to monitoring. Without such consent, an entity engaged in

---

[11] For an earlier treatment of this topic area, see Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991).

[12] Section 2511(2)(d) provides an exception to liability for an interception of a communication, stating:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior *consent* to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (2006) (emphasis added).

[13] Section 2702(b)(3) also provides an exception to liability for divulging the contents of a stored communication when consent exists. *See* 18 U.S.C. § 2702(b)(3). However, that exception only applies to an entity providing a public, not a private, service. *Id.*

the surveillance of its employees should face liability for obtaining personal information from an electronic communication. In order to give these new consent provisions effect, Congress would also have to make a few other amendments to the ECPA.[14]

Part I of this Article examines privacy and consent to monitoring of electronic communications in the workplace from an American prospective. It considers the American model of privacy protection, which advances notions of personal liberty. Part I also looks at the justifications for monitoring and the current state of protection in private and public workplaces. Part II examines privacy and consent to monitoring from a European perspective. It considers the European model of privacy protection, which advances notions of personal dignity. Part II also looks at a couple of international mechanisms that protect privacy. Part III of this Article suggests that the United States should consider the importance of dignity as a basis for privacy law. Part III further advances some amendments that would strengthen the consent provisions of ECPA, making it more consistent with the workplace dignity protections found in Europe. As a final matter, Part III stresses the importance of a default rule that protects privacy in employees' personal communications. In conclusion, this Article posits that amending ECPA to include an explicit consent provision would heighten and respect employee liberty and dignity. In so doing, the amendment would respond to the century old call of Warren and Brandeis: to find a place for dignity in American privacy law.

I. THE AMERICAN MODEL

A. Privacy as an Aspect of Personal Liberty

As mentioned previously, the United States bases its privacy rights on a strong sense of personal liberty. One can see the distinction laid out in the founding documents of this country,

[14] *See infra* Part III.B. For instance, to make any consent provision under § 2701(c) meaningful, another exception, § 2701(c)(1), would have to be eliminated for employers providing a wire or communications service to employees. *See* 18 U.S.C. § 2701(c).

especially in the Bill of Rights, with its strong circumscription of state power.[15] From the late 1700's to the present, suspicion of the government has formed the underpinning of American privacy thinking.[16] A classic statement comes from the seminal case *Boyd v. United States*,[17] where the Supreme Court noted that the Constitution provides protection from "all invasions on the part of the government . . . of the sanctity of a man's home."[18] More recently, the Supreme Court used similar language. In *Kyllo v. United States*,[19] the majority affirmed that the Constitution "draws 'a firm line at the entrance to the house.'"[20] *Boyd* and *Kyllo* illustrate how, for Americans, privacy begins with the Fourth Amendment; "at its origin, [it] is the right against unlawful searches and seizures."[21] Another recent decision, *Lawrence v. Texas*,[22] takes what seems like a dignity interest, the right to engage in private homosexual relations, and makes it one of liberty.[23] That decision begins with the statement, "Liberty protects the person from unwarranted government intrusions into a dwelling or other private places."[24] Privacy then, in the United States, means the liberty to be free from government intrusions, above all, in one's home.

United States laws suggest Americans hold much less suspicion for business entities than for the government. Most constitutional protections do not even directly apply to private businesses, except when those businesses act at the direction of the state.[25] Some federal laws and regulations create privacy rights

---

15 *See* U.S. CONST. amend. X.

16 *See* Whitman, *supra* note 4, at 1211–12.

17 Boyd v. United States, 116 U.S. 616 (1886).

18 *Id.* at 630.

19 Kyllo v. United States, 533 U.S. 27 (2001).

20 *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

21 Whitman, *supra* note 4, at 1212. Yet, "[o]ver time . . . the early republican commitment to 'privacy' has matured into a much more far-reaching right against state intrusion into our lives." *Id.*

22 Lawrence v. Texas, 539 U.S. 558 (2003).

23 *See id.* at 562; *see also* Roe v. Wade, 410 U.S. 113, 153 (1973); Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (Goldberg, J., concurring).

24 *Lawrence*, 539 U.S. at 562.

25 In order for a private entity to face liability for violating the Fourteenth Amendment and the Bill of Rights, a plaintiff must first establish that the entity acts in coordination with the government under the "state action doctrine." *See, e.g.*, The Civil Rights Cases,

against private companies;[26] however, these statutes provide spotty protections at best. Some only cover a target industry or a select class of people,[27] while others include exceptions for actions broader than conduct "in the ordinary course of business."[28] Accordingly, when private employers feel they need to monitor their employees, current laws give the employees little recourse. Government employees do not fare much better, as they only enjoy weak protections under the Constitution.

B. Factors Justifying Monitoring

Valid concerns justify some level of employer monitoring of employee electronic communications. For instance, an employee's activities through email and the Internet while on the job could create a hostile work environment for other workers. The employee might send sexually charged emails to a co-worker,[29] surf sexually explicit websites in plain view of others, or post false statements about someone. Alternatively, the employee might download unauthorized copies of music or video. In this way, employers that provide computer services could face liability for "employees' sexual, racial, or otherwise threatening or harassing

109 U.S. 3, 17 (1883); United States v. Harris, 106 U.S. 629, 638–40 (1882); Virginia v. Rives, 100 U.S. 313, 318 (1879); *see also* Pub. Utils. Comm'n v. Pollack, 343 U.S. 451, 461 (1952) (applying the state action requirement to federal constitutional claims). *See generally* Ronald J. Krotoszynski, Jr., *Back to the Briarpatch: An Argument in Favor of Constitutional Meta-Analysis in State Action Determinations*, 94 MICH. L. REV. 302 (1995). The article describes the difficult analysis required "when the actions of an ostensibly 'private' entity violate constitutional norms, and the entity enjoys some kind of special relationship or connection to the federal or a state government." *Id.* at 303.

[26] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); Wiretap Act, 18 U.S.C. §§ 2510–2522 (2006); Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2006); Pen Register Act, 18 U.S.C. §§ 3121–3127 (2006); Cable Communications Policy Act, 47 U.S.C. §§ 551–561 (2006).

[27] Notably, from the examples listed, *supra* note 26, the Cable Communications Policy Act only applies to cable operators, service providers and subscribers. *See* 47 U.S.C. § 552–561. The Children's Online Privacy Protection Act only protects children under the age of thirteen. 15 U.S.C § 6501(1).

[28] *See infra* Part I.C.

[29] Two cases come to mind in this context. In *Greenslade v. Chicago Sun-Times, Inc.*, an employee's supervisor stated in an email, "I know I'm getting to be a pain [in] the butt with these ride offers. And I apologize. But I can't help myself." 112 F.3d 853, 864 (7th Cir. 1997). In *Knox v. Indiana*, a co-worker sent an email message, asking the plaintiff if she would like to have a "horizontal good time." 93 F.3d 1327, 1330 (7th Cir. 1996).

[emails] or Internet [use] or messages, as well as for defamation, copyright infringement, fraud or other claims related to employee misconduct."[30]

The risk of losing intellectual property rights forms another important concern, justifying some level of surveillance. Trade secret law requires companies to undertake reasonable efforts to maintain the secrecy of proprietary information.[31] This information can include any "formula, pattern, compilation, program, device, method, technique, or process" that derives its value "from not being generally known to . . . other persons who can obtain economic value from its disclosure or use."[32] A trade secret loses its status as a secret, and therefore its protection, when others learn the secret without using improper means.[33] Thus, trade secret law seems to require some level of monitoring to prevent accidental or intentional breaches of secrecy.

The risks of potential liability and of losing valuable intellectual property rights act as primary motivating factors behind employer surveillance of employees.[34] While these risks do justify some level of monitoring, especially as to activities in the ordinary course of business,[35] the risks hardly justify carte blanche

---

[30] Mark E. Schreiber, *Employer E-Mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 74–75 (2000) (arguing that "[t]o deter inappropriate use and to protect themselves better, employers should implement, disseminate, and enforce e-mail and Internet use policies that are tailored to their specific business needs" and that "the policy should state the manner in which employees' business and/or personal e-mail or Internet communications can or will be accessed or monitored by the company").

[31] Particularly, a trade secret must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *See* Unif. Trade Secrets Act § 1(4) (2004).

[32] *Id.*

[33] *Id.* at § 1 cmt. ("[R]easonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on [a] 'need to know basis,' and controlling plant access.").

[34] *See* Michael L. Rustad & Sandra L. Paulsson, *Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829, 836–839 (2005) ("Monitoring [email] or Internet usage is justified, because the mishandling of these technologies is not a phantom risk.").

[35] *See* Unif. Trade Secrets Act § 1 cmt. ("The efforts required to maintain secrecy are those 'reasonable under the circumstances.' The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage.").

authority to monitor personal electronic communications made from work as "workers who [are] electronically monitored manifest[] higher rates of depression, anxiety, and fatigue than others in the same business that [are] not monitored."[36]

C. The Electronic Communications Privacy Act

In 1968, after the Supreme Court found telephone conversations subject to a reasonable expectation of privacy[37] and proposed extensive limitations on eavesdropping,[38] Congress enacted the Wiretap Act.[39] The Act criminalized private wiretaps, but allowed an exception for the wiretapping of a communication when one party consented to the tapping.[40] In 1986, Congress updated the Wiretap Act by passing the Electronic Communications Privacy Act, adding a provision to make the Act apply to the interception of electronic communications.[41] ECPA also included two new acts, the Stored Communications Act ("SCA") and the Pen Register Act. As its name suggests, the SCA protects electronic communications in storage.[42]

While the Wiretap Act and the SCA provide some protection for the electronic communications of individuals, they do little to protect employees from the surveillance of their employers

---

36 Rustad & Paulsson, *supra* note 34, at 840.

37 *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

38 *See* Berger v. State of N.Y., 388 U.S. 41, 58–60 (1967).

39 Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (codified as amended as Title I of ECPA at 18 U.S.C. §§ 2510–2522 (2006)).

40 18 U.S.C. § 2511 (2)(d).

41 Title I of ECPA, the updated Wiretap Act, defines an "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (2006).

42 Title II of ECPA, the SCA, creates civil liability for one who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a) (2006). The statute defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (2006).

because business entities receive broad exceptions under each act. For instance, Congress created service provider exceptions under both the Wiretap Act and the SCA. The Wiretap Act allows a communications service provider "to intercept, disclose, or use [a] communication in the normal course of [its] employment while engaged in any activity which is a necessary incident to the rendition of [its] service or to the protection of the rights or property of the provider of that service."[43]

The SCA's service provider exception is broader than the one found in the Wiretap Act, entirely exempting "the person or entity providing a wire or electronic communications service."[44] Another exception, the ordinary course of business exception, pertains primarily to the Wiretap Act. It limits the definition of a wiretapping device of an employer to an "electronic, mechanical, or other device" other than one used "in the ordinary course of its business."[45]

Courts have interpreted the service provider exceptions broadly in the employment context, classifying many businesses as electronic communications service providers. For instance, in *United States v. Mullins*,[46] the Ninth Circuit found that American Airlines qualified as a provider of wire or electronic communication service under § 2511(2)(a) of the Wiretap Act.[47] *Mullins* involved three travel agents' appeal from a conviction for mail and wire fraud.[48] The defendants leased computer terminals

---

43 18 U.S.C. § 2511(2)(a) (2006).

44 18 U.S.C. § 2701(c)(1) (2006).

45 This section provides:

> (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business . . . .

18 U.S.C. § 2510(5) (2006).

46 United States v. Mullins, 992 F.2d 1472 (9th Cir. 1993).

47 *Id.* at 1478.

48 *Id.* at 1474.

from American Airlines so that they could access American's electronic travel booking service.[49] American Airlines assigned the agents personal access codes and passwords, allowing them to place and edit reservations on its system.[50] After receiving notice of an anomaly on the passenger manifest of a flight returning from Europe, American Airlines personnel monitored the activity associated with the agents' codes and passwords.[51] The company then notified the FBI that it suspected the agents purposefully manipulated the passenger manifests.[52] The FBI investigated the incident, and the case went to trial.[53] At the district court, all three agents received sentences that included jail time and substantial fines.[54]

On appeal, the defendant agents argued that American's monitoring violated their Fourth Amendment rights.[55] In rejecting the agents' argument, the Ninth Circuit cited the definitions section of the Wiretap Act.[56] The court found that the service provider exception permitted American to monitor the defendants' use of its electronic travel booking service.[57] The court also found that American Airlines consented to the monitoring of its own system,[58] which qualified its surveillance for another exception under the Wiretap Act.[59]

In *Fraser v. Nationwide Mutual Insurance Co.*,[60] the Third Circuit found that the SCA provides an even broader service

---

49 *Id.* This case took place shortly before the Internet created a dearth of demand for travel agency services.

50 *Id.* at 1474–75.

51 *Id.* Due to the security atmosphere of this country following September 11, 2001, courts would probably now find an even broader exception for this type of airline computer system monitoring.

52 *Id.*

53 *Id.*

54 *Id.* ("The district court sentenced [one agent] to 48 months' imprisonment and imposed a $250,000 fine; [the second agent] received a 24-month jail term and a $15,000 fine; and [the third agent] got 21 months and a $5,000 fine.").

55 *Id.* at 1478.

56 *Id.* (citing 18 U.S.C. § 2511).

57 *Id.*; 18 U.S.C. § 2511(2)(a)(i).

58 *Mullins*, 992 F.2d at 1478.

59 18 U.S.C. § 2511(2)(d) (2006).

60 Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003).

provider exception for businesses.[61] There, the court read § 2701(c) of the SCA to "except from . . . protection *all* searches by communications service providers."[62] *Fraser* involved a wrongful termination claim brought by a former agent of Nationwide, an insurance company.[63] The plaintiff also requested damages under ECPA,[64] for violations of both the Wiretap Act and the SCA.[65] The facts of the case indicate that Nationwide believed the plaintiff was "disloyal" in his service to the company.[66] In order to substantiate this belief, Nationwide searched all of the plaintiff's email on its server, looking for email to or from the plaintiff that showed improper behavior.[67] At trial, a representative for Nationwide testified that the search proved the plaintiff's disloyalty, so Nationwide was justified in terminating him.[68] After interpreting ECPA, the district court granted summary judgment to Nationwide.[69]

The Court of Appeals for the Third Circuit affirmed the district court's decision.[70] As to the Wiretap Act claim, the Third Circuit found that the searching of email in storage did not qualify as an "interception" as required by the act because the searching did not occur contemporaneously with transmission of the email.[71] As to the SCA claim, the Third Circuit held that Nationwide fell under

61 *Id.* at 115.

62 *Id.* (emphasis added). To come to its holding, the court in *Fraser* compared the facts of the case to the facts in *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996). The *Bohach* court held that the Reno police department could, without violating the SCA, retrieve pager text messages stored on the police department's computer system because the department "is the provider of the 'service'" and "service providers [may] do as they wish when it comes to accessing communications in electronic storage." *Id.* at 1236; *Fraser*, 352 F.3d at 115.

63 *Fraser*, 352 F.3d at 109.

64 *Id.*

65 *Id.* at 113–15.

66 *Id.* at 109.

67 *Id.* at 110.

68 *Id.*

69 *Id.* at 114.

70 *Id.* at 115.

71 *Id.* at 114.

the service provider exception because it administered the email system that it searched.[72]

While not pertaining directly to electronic communications, the case *Watkins v. L.M. Berry & Co.*[73] provides a framework for interpreting the ordinary course of business exception. There, the Eleventh Circuit held that a personal communication may "be intercepted in the ordinary course of business . . . to the extent necessary to guard against unauthorized use of [equipment furnished by the business] or to determine whether the call is personal or not."[74]

In *Watkins*, the plaintiff sued her employer, alleging a violation of the Wiretap Act.[75] The circumstance of the alleged violation surrounded a personal telephone call that the plaintiff made from work to a friend, where she talked about a job interview she recently had with another company.[76] The plaintiff's employer monitored the call and approached her about it.[77] The monitoring upset the plaintiff, and eventually, she left her employer for the other company.[78] As to her Wiretap Act claim, the district court granted summary judgment on the merits to the defendant, her employer.[79]

On appeal, the parties did not dispute that the monitoring at issue violated § 2511(1)(b) of the Wiretap Act;[80] so, the Eleventh Circuit only examined whether the defendant's conduct came

---

72 *Id.* at 115. As to the SCA claim, the district court had found that the email was in "post-transmission storage." *Id.* at 114. In affirming, the Third Circuit avoided using those grounds to reach its result. *Id.*

73 Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

74 *Id.* at 583.

75 *Id.* at 579. As Congress did not pass ECPA until 1986, the plaintiff sued under the predecessor of the current Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *Id.*

76 *Id.*

77 *Id.*

78 *Id.* After tempers flared over the incident, her boss fired her. *Id.* However, she complained to another supervisor and got reinstated with apologies. *Id.* Nonetheless, the plaintiff eventually went to work for the company where she had the interview that her employer overheard her talking about. *Id.*

79 *Id.* at 579–80.

80 *Id.* at 580.

within either one of two exemptions to the Act.[81] First, the court addressed the consent exception, noting that "[c]onsent may be obtained for any interceptions" and that "the business or personal nature of the [communication] is entirely irrelevant."[82] However, the court did comment on the importance of the scope of the consent,[83] and it found that the plaintiff consented to a policy of monitoring sales calls but not personal calls.[84] As the defendant likely exceeded the scope of the consent by continuing to monitor the call after learning of its personal nature, the court found the defendant's conduct probably fell outside of the consent exception.[85]

Next, the Eleventh Circuit addressed the ordinary course of business exception. As a general rule, it noted that "if the intercepted [communication is] a business call, then . . . monitoring of it was in the ordinary course of business. If it was a personal [communication], the monitoring was probably, but not certainly, not in the ordinary course of business."[86] The court then explained, "[A] personal call may be intercepted in the ordinary

---

[81] *Id.* The Eleventh Circuit also affirmed the district court's decision to dismiss the plaintiff's claims under a duplicative provision of the Communications Act. *Id.*

[82] *Id.* at 581 (noting that as long as the requisite business connection is demonstrated, the business extension exemption represents the "circumstances under which non-consensual interception" does not violate section 2511(1)(b) (citing Briggs v. Am. Air Filter Co., 630 F.2d 414, 419 (5th Cir.1980))).

[83] *Watkins*, 704 F.2d at 582. The Eleventh Circuit noted:

> We can think of no reason why consent under [the Wiretap Act] cannot be limited. We therefore hold that consent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be limited. It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent.

Id.

[84] *Id.* at 581.

[85] *Id.* at 582. However, the Eleventh Circuit did direct the district court to settle the factual issues surrounding the consent on remand. *Id.* at 585 ("Among the factual questions that should be considered are: What was the monitoring policy to which Watkins consented?").

[86] *Id.* at 582 ("The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company. Such a broad reading 'flouts the words of the statute and establishes an exemption that is without basis in the legislative history' of [the Wiretap Act]." (quoting Campiti v. Walonis, 611 F.2d 387, 392 (1st Cir. 1979))).

course of business to determine its nature, but never its contents."[87] Yet, instead of holding for the plaintiff, the Eleventh Circuit remanded to the district court, charging it to determine whether the plaintiff's employer learned of the plaintiff's job interview during a permissible window of interception.[88] While the court suggested the permissible window for determining the nature of a call was less than three minutes, it left that determination to the trial court.[89]

Of the three cases described above, only *Watkins* draws a line between the interception of communications to protect legitimate business interests and the interception of purely personal communications, making the latter a likely violation of the Wiretap Act.

In *Mullins*, the Ninth Circuit may have rightly found that the monitoring conducted by American Airlines did not violate ECPA;[90] however, the court did so without determining the scope of permissible monitoring. Perhaps American Airlines should receive an exemption under ECPA for monitoring fraudulent activities on its system because fraud represents an affront to American's legitimate business concerns, but that exemption should not broadly stem from it providing a wire or electronic communication service. Additionally, to the extent the analysis in *Mullins* suggests that the party conducting the monitoring of an employee or agent can consent to the monitoring itself,[91] the decision presents an unworkable interpretation of ECPA, effectively eviscerating the statute's protections.

The decision reached by the Third Circuit in *Fraser* suffers from greater problems. The court's interpretation of the Wiretap Act places all employee email communications under the sole protection of the SCA.[92] This solution is problematic because an employer can avoid reading an email "contemporaneous with

---

87 *Id.* at 583.

88 *Id.* at 584.

89 *Id.* at 584. "It has been widely advertised that one may reach out by telephone and touch all sorts of people in 3 minutes or less; it seems to us that it should not take that long to determine whether a call is of a personal or a business nature." *Id.* at 585 n.10.

90 *See supra* notes 46–58 and accompanying text.

91 United States v. Mullins, 992 F.2d 1472, 1472 (9th Cir. 1993).

92 Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003).

transmission," and instead, it can resort to a stored copy of the email.[93] The *Fraser* court's interpretation of ECPA would not necessarily harm the privacy interests of employees if it were not for the blanket immunity the courts give business entities for searches of stored communications they conduct on email systems they provide. Absent from the court's analysis was whether ECPA restricts the scope of the search to communications in which the employer has a legitimate business concern.

Even the analysis in *Watkins* presents some troubling implications. There, the Eleventh Circuit suggested that the scope of consent should have limitations and that consent "is not to be cavalierly implied;"[94] however, the court did, in fact, imply consent. The court found that a stated policy of monitoring sales calls, along with the plaintiff's knowledge of the policy when she accepted employment, created consent to the monitoring of sales calls.[95] Thus, the analysis of *Watkins* allows a loophole through which businesses can escape all liability under ECPA. An employer need only have a stated policy, to which an employee need not even explicitly convey consent, that it may monitor all business and personal calls.

D. The Lack of Safeguards under the Fourth Amendment

As mentioned earlier, employees working for private employers receive little help from the Constitution because it "erects no shield against merely private conduct, however discriminatory or wrongful."[96] Particularly, the Fourth Amendment "does not protect against a search or seizure by a private party on its own initiative, even if the search or seizure is an arbitrary action."[97] However, despite their constitutional protections, government employees fare little better than private employees when subjected to monitoring by their employers.

---

93 *See supra* notes 60–72 and accompanying text.

94 Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

95 *Id*.

96 Shelley v. Kraemer, 334 U.S. 1, 13 (1948).

97 Baggs v. Eagle-Picher Indus., Inc., 750 F. Supp. 264, 271 (W.D. Mich. 1990).

O'Connor v. Ortega[98] illustrates how little constitutional protection government employees receive when their employers monitor or search their personal communications. There, the Supreme Court found that "a probable cause requirement for searches . . . would impose intolerable burdens on public employers."[99]

In *Ortega*, the plaintiff, a physician and psychiatrist, filed suit under 42 U.S.C. § 1983, alleging that his employers had violated the rights provided to him under the Fourth Amendment.[100] The potential Fourth Amendment violation stemmed from a search that the plaintiff's employer conducted.[101] The plaintiff's supervisor, the executive director of the public hospital where he worked, suspected that the plaintiff had engaged in improprieties while running the hospital's residency program.[102] In order to substantiate his suspicions, the executive director placed the plaintiff on administrative leave and appointed a team to conduct an investigation of the plaintiff's activities.[103] The leader of the investigative team decided to conduct a thorough search of the plaintiff's office while he was away.[104] The team entered the office a number of times and seized some of the plaintiff's personal items from his desk and file cabinet.[105] After the team concluded its investigation, the hospital terminated the plaintiff's employment.[106]

In considering whether the above search violated the plaintiff's Fourth Amendment rights, first the Court determined whether the plaintiff had a reasonable expectation of privacy in his office.[107] The undisputed evidence disclosed that the plaintiff did not share

---

98 O'Connor v. Ortega, 480 U.S. 709 (1987).

99 *Id.* at 724.

100 *Id.* at 714.

101 *Id.* at 713.

102 *Id.* at 712–13.

103 *Id.*

104 *Id.* at 713.

105 *Id.* These items included a Valentine's Day card, a photograph, and book of poetry. *Id.* A former resident physician had sent these items to the plaintiff, and, at a hearing before the state personnel board, the plaintiff's employer used them to impeach her credibility when she testified on the plaintiff's behalf. *Id.*

106 *Id.*

107 *Id.* at 715–16.

his desk or file cabinets with any other employees and that he kept only personal communications and communications with patients unconnected with the hospital in his office, along with his personal financial records and some personal gifts and mementos.[108] Notably, the plaintiff did not keep any files on physicians in residency training in his office.[109] Thus, the Court found the plaintiff had a reasonable expectation of privacy in his desk and file cabinet.[110]

Next, the Court turned to what procedural hurdles it should place before a public employer that, once passed, would make its search of an employee's protected space lawful. Citing *New Jersey v. T.L.O.*,[111] the Court noted, "[only] in those exceptional circumstances in which special needs . . . make the warrant and probable-cause requirement impracticable" should the court abrogate that standard.[112] However, the Court seemingly skipped the special needs analysis,[113] summing up its position in a statement that "[i]t is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard."[114] Thus, the Court held that "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct,

---

[108] *Id.* at 718.

[109] *Id.*

[110] *Id.* at 719. However, the Court noted:

> Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practice and procedures, or by legitimate regulation . . . . The employee's expectation of privacy must be assessed in context of the employment relation . . . . [S]ome government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable.

Id. at 717–18.

[111] New Jersey v. T.L.O., 469 U.S. 325 (1985).

[112] *Ortega*, 480 U.S. at 720 (alteration in original).

[113] Justice Blackmun, writing for the dissent, noted, "[a]lthough the plurality mentions the 'special need' step, . . . it turns immediately to a balancing test to formulate its standard of reasonableness." *Id.* at 742 (Blackmun, J., dissenting). He further stated, "This error is significant because, given the facts of this case, no 'special need' exists here to justify dispensing with the warrant and probable-cause requirements." *Id.*

[114] *Id.* at 724–25 (majority opinion).

should be judged by the standard of reasonableness under all circumstances."[115] The Court articulated the standard of reasonableness as conduct "according to the dictates of reason and common sense."[116]

The level of Fourth Amendment protection in the workplace set by the Court in *Ortega* shows noticeable weaknesses. First, an employee must prove a reasonable expectation of privacy in the area searched, instead of in the communication apprehended, which is no easy task. Not all employees enjoy the comfort of private offices as the plaintiff in *Ortega* did. Second, an employee must prove any monitoring was unreasonable, a circumstance much harder to show than a lack of probable cause. As their constitutional remedy only weakly protects them in the workplace, public employees, like private employees, could use a more effective statutory remedy. In contemplating one, Congress should consider the statutory privacy protections that European countries provide their citizens.

II. THE EUROPEAN MODEL

A. Privacy as an Aspect of Personal Dignity

Unlike the core foundation of American privacy law, largely concerned with personal liberty, European privacy law focuses more on protecting aspects of personal dignity.[117] Why does Europe strive to protect and guarantee certain levels of respect, social esteem, and personal honor for its citizens? From the point of view of many Europeans and Americans, laws protecting one's dignity came as a reaction against the indignities perpetrated in the name of fascism, especially Nazism.[118]

On the one hand, that explanation may oversimplify the evolution of privacy law in Europe, for, as Warren and Brandeis

---

115 *Id.* at 725–26.

116 *Id.* at 725 (quoting New Jersey v. T.L.O., 469 U.S. 325, 343 (1985)).

117 *See* Whitman, *supra* note 4, at 1164 ("The political and social values of 'dignity' and 'honor' are indeed what is at stake in the [European] concept of privacy.").

118 *See id.* at 1165. *See generally* ROBERT KAGAN, OF PARADISE AND POWER: AMERICA AND EUROPE IN THE NEW WORLD ORDER (2003).

recognized,[119] the history of European laws protecting dignity began long before the postwar period.[120] On the other hand, the postwar period did play an important role in creating modern European dignity rights, much as the Revolutionary War played its role in fostering American liberty rights. Before the Second World War, only high-status persons could expect to have the courts protect their personal honor,[121] while members of lower classes lived their lives without a meaningful right to respect.[122] Throughout the past seventy years, average Europeans have "leveled-up" to experience, many, if not all, of the rights once held only by the former ruling class.[123] Now all citizens of Europe's core states may experience protections for their personal reputation and personal information.[124]

To be sure, the American system of liberty protection is not without its advantages over the European system of dignity protection. Unlike the United States, where privacy means protection from state intrusion, governments in Europe accomplish a remarkable level of surveillance with little or no uproar from their citizenry.[125] Further, in Europe, governments enforce some dignity norms that Americans would find absurd, perhaps even an affront to their liberty.[126] The European laws regulating childrens'

---

[119] Warren & Brandeis, *supra* note 1, at 214, 214 n.1 (adapting notions of French privacy law to limit the breadth of a tort against invasion of privacy: "The right to privacy, limited as such a right must necessarily be, has already found expression in the law of France").

[120] Whitman, *supra* note 4, at 1165–66.

[121] *Id.* at 1170–71. A disproportion of concern for royalty in European privacy thinking still exists. For instance, "German texts list royalty first among the classes of 'public figures' who require special treatment in the law of privacy, while French texts . . . only list royalty second, after politicians." *Id.* at 1169–70.

[122] James Q. Whitman, *Enforcing Civility and Respect: Three Societies*, 109 YALE L.J. 1270, 1320–30 (2000).

[123] *See* Whitman, supra note 4, at 1164–71 ("This long term secular leveling-up tendency has shaped [European] law in a very fundamental way.").

[124] *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[125] "In Germany, everybody must be formally registered with the police at all times." Whitman, *supra* note 4, at 1158. Further, in France and Germany, "telephones are tapped at ten to thirty times the rate they are tapped in the United States—and in the Netherlands and Italy, at 130 to 150 times the rate." *Id.* at 1159. However, as others have noted, "The [United States] is far more predisposed to subordinate privacy to security than the Europeans are." Rustad & Paulsson, *supra* note 34, at 865.

[126] *See* Whitman, *supra* note 4, at 1158.

birth-names stand as but one example.[127] Thus, in some ways, European regulation of dignity rights may go too far. However, one can hardly argue that, by obliging their bosses to respect the privacy of their personal electronic communications in the workplace,[128] Europeans do not confirm in themselves at least a somewhat heightened sense of personhood.

B. Article 8 of the Convention for the Protection of Human Rights and Directive 95/46/EC

Shortly after beginning to recover from the devastating and costly Second World War, the countries of Europe gathered to draft legislation, which would protect the region from further human rights atrocities.[129] The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 ("ECHR") resulted from their combined efforts, and it now forms a legal standard that each member state of the European Union has incorporated into its national laws.[130] The European Court of Human Rights enforces the protocols of the ECHR;[131] individuals appeal to the court as an applicant when they have exhausted their domestic remedies, receiving a judgment binding on both the individual and the respondent state.[132]

Europeans enjoy some significant privacy protections under the ECHR. Article 8 of the ECHR specifically defends the right one has "to respect for his private and family life, his home, and his correspondence."[133] The European Court of Human Rights extended the definition of "private life" to include the right to protection for one's personal matters in certain business environments, and it expanded the definition of "correspondence" to include email and other electronic communications.[134]

---

127 *Id.*

128 *See infra* Part II.B. European law also protects "the right of workers to respectful treatment by their bosses and coworkers." Whitman, *supra* note 4, at 1165.

129 *See* Rustad & Paulsson, *supra* note 34, at 871.

130 *Id.*

131 *Id.*

132 *Id.* at 872.

133 Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

134 Rustad & Paulsson, *supra* note 34, at 872.

For instance, in *Niemietz v. Germany*,[135] the European Court of Human Rights thought it too restrictive to limit the notion of "private life" to an "inner circle" where an individual may live as he chooses, excluding from the definition everything outside that circle.[136] Instead, the court found that "private life" may include "activities of a professional or business nature"[137] because, at times, one may not be able to distinguish clearly whether "an individual's activities form part of his personal or business life."[138]

Niemietz involved a search of the law office premises of the applicant, Mr. Niemietz, to find information relevant to a crime of insult, an illegal act in Germany.[139] The authorities used a warrant to conduct the search, trying to discover the author of an offensive letter, which constituted the insult.[140] The court found that the "search impinged on [applicant's] secrecy to an extent . . . disproportionate [under] the circumstances,"[141] thus, it concluded that the search resulted in a breach of Article 8 of the ECHR.[142] However, finding an absence of damages, the court dismissed applicant's claim for just satisfaction.[143]

In another case, *Halford v. United Kingdom*,[144] the European Court of Human Rights applied Article 8 of the ECHR to the interception of personal phone calls at work. It found "telephone calls made from business premises as well as from the home may

---

135 Niemietz v. Germany, 251 Eur. Ct. H.R. 23 (1992).

136 *Id.* ¶ 29 ("Respect for private life must also comprise to a certain degree the right to establish . . . relationships with human beings.").

137 *See id.* ("[I]t is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with [people].").

138 *Id.*

139 *Id.* ¶¶ 6–16.

140 *Id.* ¶ 10.

141 *Id.* ¶ 37 (expressing concern that "the attendant publicity must have been capable of affecting adversely the applicant's professional reputation, in the eyes of both his existing clients and of the public at large").

142 *Id.* ¶ 38.

143 *Id.* ¶ 43 ("[A]lthough Mr. Niemietz stated at the hearing that his request extended to his costs and expenses referable to the proceedings . . . he has supplied no particulars of that expenditure.").

144 Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).

be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8."[145]

In *Halford*, the applicant, an assistant chief constable, complained that her employer, the Merseyside Police Authority, intercepted calls made from her office telephone.[146] Prior to the monitoring, she had sued the police department for sexual harassment, as the authority had denied her several promotions.[147] Before the European Court of Human Rights, the United Kingdom government, representing the view of the police authority, submitted that telephone calls one makes from the workplace fall outside the protection of Article 8.[148] The court disagreed and held that the telephone calls applicant made sat "within the scope of 'private life' and 'correspondence.'"[149] In its decision, the court noted that the police authority had not explicitly told applicant her calls would be liable to interception and that this gave applicant a "reasonable expectation of privacy" in those calls.[150] The decision in *Halford* posits an interesting solution to the problem of employee monitoring. It suggests that such monitoring will not violate Article 8 if the employer achieves express notice and consent from its employee.[151]

Europeans receive another layer of protection from monitoring through European Council Directive 95/46 ("Directive 95/46/EC" or "the Directive"),[152] the directive on the protection of personal data. "Directive 95/46/EC establishes a 'minimum framework' of data protection requirements,"[153] which each member state of the European Community implemented into law. "These requirements

---

145 *Id.* ¶ 44.

146 *See id.* ¶17.

147 *See id.* ¶¶ 10–11.

148 *See id.* ¶ 43 ("At the hearing before the Court, counsel for the Government expressed the view that an employer should in principle, without prior knowledge of the employee, be able to monitor calls made by the latter on telephones provided by the employer.").

149 *Id.* ¶ 46.

150 *Id.* ¶ 45.

151 *Id.* ¶ 44.

152 Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

153 Lothar Determann et al., *Global Data Transfers and the European Directive A Practical Analysis of the New ICC Contract Clauses*, 4 PRIVACY & SECURITY L. REP. 153, 154 (2005).

apply to any collection, use, disclosure, or other processing of information about an identified or identifiable natural person in the [European Economic Area]."[154] "[T]he definition of 'processing of personal data' set out in Article 2 of Directive 95/46/EC also covers all forms of computer surveillance," including the monitoring of personally identifiable electronic communications.[155] Thus, the Directive has omnibus scope, and it "applies broadly to all industries and business sectors," both private and public.[156] It certainly applies to monitoring in the workplace.[157]

Article 7 of the Directive states, "Member States shall provide that personal data may be processed only if" the processing meets one of six exceptions.[158] Exception (a), the most important exception for the sake of this Article, allows data processing when "the data subject has unambiguously given his consent."[159] Article 2 of the act further defines consent as "any freely given and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[160] Thus, these provisions require consent that is "freely given, specific and informed."[161] Under this conception of consent, any employer that wishes to monitor its employee must notify the employee of the nature and purpose of the monitoring, which must be specific and not over-general, and then it must achieve express consent.[162]

Taken together, the ECHR and Directive 95/46/EC give significant protections to both private and public employees in Europe. By experiencing privacy as to their personal

---

154 *Id.*

155 Roberto F. Filho & Mark Jeffery, *Information Technology and Workers' Privacy: Notice and Consent*, 23 COMP. LAB. L. & POL'Y J. 551, 554 (2002).

156 *See* Determann et al., *supra* note 153, at 154.

157 *See* Filho & Jeffery, *supra* note 155, at 562–67.

158 Council Directive 95/46, art. 7, 1995 O.J. (L 281) 31, 40 (EC).

159 *Id.*

160 Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 39 (EC).

161 *See* Filho & Jeffery, *supra* note 155, at 564.

162 *See id.* at 564–65 ("[T]here remains a considerable margin of doubt . . . over the closely-related question of whether consent must be given every time the employer 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.").

communications and data at work, Europeans may, indeed, feel more dignified in the workplace. But, are their liberty interests more protected?—Arguably not. Enforcement of Article 8 of the ECHR against government authorities acting pursuant to protocol suffers from noticeable weaknesses,[163] and Directive 95/46/EC entirely exempts processing "necessary for compliance with a legal obligation."[164] Further, in some ways, both schemes for protecting privacy may go too far. Neither the ECHR nor the Directive has a clearly articulated exemption for employee monitoring an employer undertakes in the ordinary course of business, and as discussed above, some instances do exist that justify employee monitoring. Therefore, this Article does not advance that the United States should engage in the full-scale adoption of European protections for electronic communications. The United States may, however, take something of value from the work-place privacy protections implemented by its neighbors across the Atlantic.

III. REDEFINING CONSENT: RECOGNIZING LIBERTY AND DIGNITY

A. The Importance of Dignity

Professor Bloustein, a noted privacy scholar, once wrote, "[A]nalysis of the interest involved in . . . privacy cases is of utmost significance because in our own day scientific and technological advances have raised the spectre of new and frightening invasions of privacy."[165] His statement confronted a pressing reality that is ever more true today, especially in the workplace. In 2004, a survey of employer monitoring confirmed that 74% of responding companies monitor the outgoing and incoming email of their employees and that 60% monitor

[163] For instance, in *Niemietz*, even after finding the warrant at issue faulty, the court did not award the applicant any just compensation. *See* Niemietz v. Germany, 251 Eur. Ct. H.R. 23 (1992); *supra* notes 135–43 and accompanying text. Perhaps that is why *Niemietz* and *Halford* number among the select few cases addressing Article 8 of the ECHR in the last twenty years.

[164] Council Directive 95/46, art. 7, 1995 O.J. (L 281) 31, 40 (EC).

[165] Bloustein, *supra* note 7, at 963.

employee Internet connections.[166] Further, as Justice Blackmun noted in his dissent in *Ortega*, "It is, unfortunately, all too true that the workplace has become another home for most working Americans. . . . Consequently, an employee's private life must intersect with the workplace."[167]

When confronted with these actualities, perhaps then, all Americans should respond as Professor Bloustein did. In his 1964 article, *Privacy as an Aspect of Human Dignity*, he explained that just as we may regard these intrusions "as offensive to our concept of individualism and the liberty it entails, so too should we regard privacy as a dignitary [injury]."[168] In other words, the United States needs to consider laws that protect privacy not only as an aspect of liberty, but also as an aspect of dignity. By implementing the changes to ECPA that this Article suggests below, Congress may be able to accomplish that goal for employees in the workplace.

Before considering a change to ECPA, which would increase its dignity protections, however, this Article must address one last aspect of liberty that comes into play with business entities: freedom of contract. In the past, the Supreme Court struck down laws limiting freedom of contract in the employer/employee context, characterizing the dispute as a conflict between "the power of the State to legislate or the right of the individual to liberty."[169] While some of the cases espousing freedom of contract

---

[166] *See* Reginald C. Govan & Freddie Mac, *Workplace Privacy*, *in* 33RD ANNUAL INSTITUTE ON EMPLOYMENT LAW 245, 251 (Practising Law Institute 2004) (noting the study also "found a positive correlation between the size of the company and its level of monitoring and surveillance, with the largest companies conducting the most surveillance").

[167] O'Connor v. Ortega, 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting).

[168] *See* Bloustein, *supra* note 7, at 1002 (speaking of the torts protecting privacy). Bloustein also noted, "The right to privacy in the form we know it, however, had to await the advent of the urbanization of our way of life . . . because only then was a significant and everyday threat to personal dignity . . . realized." *Id.* at 984.

[169] *See, e.g.*, Lochner v. New York, 198 U.S. 45, 57 (1906). In *Lochner*, the Supreme Court considered a statute that restricted the power of employers to require their employees, in this case bakers, to work over sixty hours a week. *Id.* at 52–53. The Court saw the statute as unconstitutional, noting:

> The statute necessarily interferes with the right of contract between the employer and employees, concerning the number of hours in which the latter may labor in the bakery of the employer. The

as a fundamental right fell into disfavor during the New Deal, freedom of contract remains an aspect central to the American idea of liberty. As European courts hold little respect for contracts signed in the employment context,[170] any consideration of European dignity protections will have to ignore that aspect of European law; it is too incompatible with American ideals.

B. Looking to Europe for Help in Amending ECPA

In suggesting a change to American law to increase dignity protections, this Article looks across the Atlantic to those countries more familiar with privacy as an aspect of dignity, just as Warren and Brandeis did in their privacy article. Yet this Article does not propose to completely do away with the statutory scheme already in place. Instead, it posits that, with only small changes, ECPA can provide for worker dignity and allow for justified employer monitoring. Employees need a more robust ECPA because, for private employees, it forms one of the only protections they have. Public employees would benefit too, since they receive little protection from the Fourth Amendment.

As the first amendment to ECPA, Congress should eliminate employer eligibility for the service provider exceptions in both the Wiretap Act under 18 U.S.C. § 2511(2)(a)[171] and the SCA under 18 U.S.C. § 2701(c)(1),[172] when the case concerns monitoring of an employee. As illustrated above, courts have interpreted these exceptions in such a way as to make other exceptions, such as consent, redundant and meaningless.[173] The SCA's service provider exception stands as the prime example.[174] Most

> general right to make a contract in relation to his business is part of the liberty of the individual protected by the Fourteenth Amendment of the Federal Constitution (citation omitted). Under that provision no State can deprive any person of life, liberty or property without due process of law.

Id. at 53.

170 *See* Determann et al., *supra* note 153, at 156.

171 *See supra* note 43 and accompanying text.

172 *See supra* note 44 and accompanying text.

173 *See supra* Part I.C.

174 Remember, this exemption was read by the Third Circuit to "except from [the SCA's] protection all searches by communications service providers." Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003).

employers provide email and Internet service to their employees, and classifying these employers as service providers when they do so exempts them from the SCA, leaving them free to monitor their employees without regard to whether the monitoring addresses a legitimate business concern.

As a second amendment to ECPA, Congress should implement the ordinary course of business exception as defined by the court in *Watkins* for both the Wiretap Act and the SCA.[175] For the Wiretap Act, this would mean adding additional provisions to the current exception under 18 U.S.C. § 2510 (5)(a).[176] For the SCA, this would mean creating an entirely new exemption under 18 U.S.C. § 2701(c).[177] The ordinary course of business exception should entitle an employer only to monitor the communications of an employee if the communication pertains to a legitimate business concern. As explained by *Watkins*, this exception must have limited scope;[178] there must be minimization of the harm to the employee's dignity.

The minimization requirement of the statute should provide for the following contingencies. If an employer seeks to monitor a communication to find out whether it is business related or personal, the employer must immediately cease monitoring when it discovers the communication is indeed personal. In the context of personal telephone communications, an employer should not listen for more than three minutes before ceasing to monitor the call.[179] In the context of email communications, an employer should not review more than the subject line of the email. In the context of Internet usage, an employer should, as in the phone context, not examine more than three minutes of usage, whether the usage is intercepted or stored. All of these limits should apply during a

---

175 *See supra* notes 73–85 and accompanying text.

176 Currently, the exception listed here does not require minimization, as *Watkins* does. *See* Watkins v. L.M. Berry & Co., 704 F.2d. 577, 583–84 (11th Cir. 1983).

177 The ordinary course of business exception for employers could replace the service provider exception currently found in 18 U.S.C. § 2701(c)(1).

178 *See Watkins*, 704 F.2d. at 583–84.

179 Three minutes is the length of time used by the court in *Watkins*. *See id.* at 585. Upon further analysis of the time it takes to determine if a call is business or personal, this three minute limit could be revised.

calendar day. That is, employers should only be able to take one "peak" per day.

This minimization requirement raises another concern, which may warrant an additional "poisonous fruits" provision. Employers may attempt to benefit from personal information they overhear even when they abide by the guidelines set out above. Thus, Congress should limit the use of any personal information "accidentally" attained while an employer "peaks" to see if the communication is for business or personal reasons. Congress should also limit the use of any personal information attained while monitoring a communication in the ordinary course of business,[180] unless the personal information is inseparably intertwined with a legitimate business purpose. Moreover, misuse of personal information should constitute a violation of ECPA.

As the final, and most important, amendment, Congress should alter the consent provisions of the Wiretap Act and the SCA. As discussed above, freedom to contract forms a central aspect of American liberty, and as such, Congress should not eliminate the provision altogether. However, current interpretations of consent to monitoring of personal communications in the workplace create an unworkable and undignified solution. How can an employee freely contract when a court implies the employee's consent, or rather, finds the consent of another adequate?[181] In order to preserve the bargaining power of an employee, and therefore the employee's dignity and liberty, Congress should adopt some of the consent provisions of Directive 95/46/EC.

In amending the consent provision of 18 U.S.C. § 2511(2)(d) and adding a similar consent provision to § 2701(c), Congress should require that any consent to monitoring of personal communications be freely given, specific, and informed.[182] It

[180] Some business communications, undoubtedly, contain personal information, as many people engage in business relationships with their personal friends or become personal friends with those they engage in business with.

[181] *See supra* notes 94–95 and accompanying text.

[182] *See supra* note 161 and accompanying text; Council Directive 95/46, art. 2, 1995 O.J. (L 281) 31, 39 (EC).

should also be explicit and unambiguous.[183] In practice, this means that an employee should have full notice of the scope of and the justifications for the monitoring of personal communications. Full notice would be beneficial because the alternative, "widespread individual ignorance[,] hinders development through the privacy marketplace of appropriate norms about personal data use."[184] The employer should give the employee a form detailing the extent of the monitoring for the employee to sign. The form should have no other provisions than those dealing with the monitoring of personal, non-business, communications. The employer should ask the employee—orally, not in writing—if the employee understands the provisions, and the employer should offer further explanation, if necessary. Last, the employee should have to sign the form next to a statement of explicit consent for the monitoring of the employee's personal communications.

All of the above-mentioned steps may sound tedious, and they are. However, one must remember that the amendments this Article suggests would also reaffirm an ordinary course of business exception to monitoring. The above stated consent exception would apply only to personal communications, allowing an employee to ask why the employer feels it necessary to monitor personal communications. Its specificity requirement would limit the scope of monitoring to the extent the employer can justify. Moreover, the consent exception would provide a bargaining point in employment negotiations. If an employer feels it must monitor extensively to protect itself, perhaps it will have to pay its employees a little more.[185]

This Article needs to address one last aspect of the consent exception for ECPA: the default rule.[186] That is, in the absence of explicit consent, what will the rule be? A simple answer to that

---

[183] *See supra* note 159 and accompanying text; Council Directive 95/46, art. 7, 1995 O.J. (L 281) 31, 40 (EC).

[184] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1683 (1999).

[185] *Id.* at 1681–91; *cf.* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246–47 (1998).

[186] Jerry Kang has addressed the importance of default rules. *See* Kang, *supra* note 185, at 1247–59 ("Unless the parties agree otherwise, the information collector should process personal data only in functionally necessary ways.").

question exists: in the absence of consent, either employer interception of personal communications or employer access of stored personal communications will violate ECPA. Besides the ordinary course of business exception, no other exception would apply.[187] In this way, the default rule presents employees with a choice, and freedom to choose would enhance both the liberty and the dignity of the employee.[188]

Some might argue that "high transaction costs may convert this 'default' rule into a practically 'immutable' rule."[189] For instance, on the one hand, a small employer may not have the infrastructure to secure informed consent. In that case, all employees would enjoy the full protections under ECPA for their personal communications. Large companies, on the other hand, will likely have the infrastructure to secure consent. However, cost cutting across the business as a whole will encourage such a company to restrict its monitoring to the extent it is necessary,[190] especially if employees argue for higher pay to counter the intrusion into their personal lives.

C. Responding to Warren and Brandeis' Call

In the conclusion of their article, *The Right to Privacy*, Warren and Brandeis commented, "[L]aw has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands."[191] Then the two authors rebuked, "Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?"[192]

In the terms of this Article, Warren and Brandeis seem to have suggested: Why should the law only protect one's privacy as an

---

[187] That is, no other exception would apply for employer use of the information. Government use may still be excepted under other provisions.

[188] *See* Kang, *supra* note 185, at 1259–65 ("[S]urveillance is in tension with human dignity.").

[189] *Id.* at 1250.

[190] *Id.* at 1250–51 ("[E]ven if transaction costs are not large enough to transform default rules into immutable ones, the default rule still matters because 'it determines who will bargain and at what cost.'").

[191] Warren & Brandeis, *supra* note 1, at 220.

[192] *Id.*

aspect of liberty—freedom from the intrusion of the state in one's own home, when it could also protect privacy as an aspect of dignity—freedom from the intrusion of everyone, including the state, in one's personal affairs? While each side of the Atlantic may view liberty or dignity as the core inviolable right subject to privacy protection, perhaps here in the United States we can enhance our dignity protections without sacrificing our liberty or the concerns of our businesses. By amending ECPA, Congress may be able to accomplish just such an ideal for American employees, protecting privacy as an aspect of liberty and dignity.