SMU Science and Technology Law Review

Volume 26 | Number 1 Article 9

2023

Employee Monitoring: As Technology Advances Yet the Electronic Communications Privacy Act Stays in the Past

Isabela Possino
Southern Methodist University, Dedman School of Law

Employee Monitoring: As Technology Advances Yet the Electronic Communications Privacy Act Stays in the Past

*Isabela Possino**

ABSTRACT

Since the Electronic Communications Privacy Act of 1986 was enacted, the United States has endured an evolution of technology. While progressive at its inception, the ECPA has since been met with a tumultuous response from scholars, courts, and others trying to understand its purpose and application regarding privacy rights and the monitoring of communications. Specifically, since the COVID-19 pandemic, the ECPA has remained at the forefront of debate with respect to employee monitoring and surveillance practices. This article provides an overview of the ECPA and explains why today's technological advancements have surpassed the protections afforded by the Act, leaving employees at risk and employers with significant discretion to implement their desired monitoring practices. While initially intended to extend privacy protections for U.S. citizens, the Act carved out various exceptions for which monitoring is permitted, including most business-related purposes. In addition, this article discusses the approaches and legislation that several states have proposed to combat the ambiguities of the ECPA and highlights the various ways the federal government could amend the ECPA to resolve such challenges and protect the privacy rights of employees in U.S. companies.

I. INTRODUCTION

As the average American workday continues to evolve both in environment and in expectation, concerns related to employee data privacy and employer monitoring practices continue to grow, yet U.S. statutes and regulations remain the same.[1] In particular, though the Electronic Communications Privacy Act (ECPA) of 1986 was enacted to address technology that had developed in the 1980s, significant technological advancements such as the internet, social media, and personal devices have emerged since.[2] While the ECPA has been amended four times since its inception, the legislature

DOI: https://doi.org/10.25172/smustlr.26.1.9.

* Isabela Possino is a 2024 candidate for Juris Doctor from SMU Dedman School of Law. She received Bachelor of Arts degrees in Political Science and Psychology from Pennsylvania State University in 2021.

1. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1243 (2004).

2. *See* Thomas Reuters Editorial Staff, *Employee Monitoring*, 38-18 LAW.'S BRIEF ART. I 1, 1 (2008).

has not yet addressed the capabilities of new technology nor monitoring systems, leaving the rights intended to protect United States citizens unclear.[3]

In the absence of any new federal regulations, states have enacted their own statutes.[4] For example, following the practices in neighboring states, New York enacted the Employee Monitoring Notice Law in November of 2021.[5] The Act addresses electronic monitoring and requires employers who engage in monitoring to provide notice of such practices to their employees.[6] By contrast, Texas employers are not required to provide notice of monitoring and are instead generally free to monitor their employees with few restrictions.[7]

Thus, state regulations leave employers with either complete discretion in their monitoring practices or minor restrictions, and employees are left with narrow protections varying from state to state.[8] This case note seeks to address this issue in three parts. The first part will provide an explanation and overview of the Electronic Communications Privacy Act of 1986 and its application to employee monitoring and surveillance practices. The second part will explain how advancements in technology and the evolution of the workplace environment have outgrown the ECPA, requiring updated legislation. Finally, the third part will discuss both the legal implications that arise from the wide range of discretion given to employers while the Electronic Communications Privacy Act remains unamended and offer various ways the legislature could amend the ECPA to resolve its ambiguities and challenges.

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND ITS APPLICATION TO EMPLOYEE DATA

A. What is the ECPA?

In order to understand the Electronic Communications Privacy Act, it is important to understand its purpose, scope, and relative decisions.[9] The Electronic Communications Privacy Act (ECPA) of 1986 was enacted to expand the Federal Wiretap Act of 1986 and extend privacy protections to certain technological advancements that emerged after the Act's inception.[10] Prior to

3. *See* Ariana R. Levison, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 464 (2012).

4. Thomas Reuters Editorial Staff, *supra* note 2, at 15.

5. S. B. 2628, 2021 Leg., Reg. Sess. (N.Y. 2021) (enacted).

6. *Id.*

7. Andrew Milam Jones, *Employee Monitoring: An Overview of Technologies, Treatment, and Best Practices*, 83 Tex. Bar J. 1, 98 (2020).

8. *See id.* at 99.

9. *See* 18 U.S.C.A. § 2510 (West 2002).

10. Thomas Reuters Editorial Staff, *supra* note 2, at 1.

the ECPA, only oral communications such as telephone conversations were protected, as the Federal Wiretap Act covered only communications "heard and understood by the human ear."[11] However, with the ECPA, federal protections grew to include "wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers."[12]

B. How the ECPA Applies to Employee Monitoring

The ECPA is divided into three titles.[13] However, only Title I and Title II are of relevance to the protections of employee communications.[14] Title I of the ECPA, often referred to as the Wiretap Act, deals with communications in transit and prohibits the intentional "intercept[ion], endeavor to intercept, or procure[ment of] any other person to intercept" a protected communication.[15] An interception, as defined by the Wiretap Act, includes "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."[16] Thus, under the Wiretap Act, the act of monitoring or accessing another citizen's oral, electronic, or wire communications is generally prohibited.[17]

Title II of the ECPA, coined the Stored Communications Act (SCA), prohibits any individual or entity from intentionally accessing unauthorized stored communications or exceeding an authorization to access stored communications.[18] Through the Stored Communications Act, the ECPA regulates and limits the ability of government officials, individuals, and corporate entities to access stored communications.[19] Thus, an individual who intentionally and without authorization accesses a database containing electronic communications would be in violation of the Stored Communications Act.[20]

However, there are significant exceptions to the rights protected within the Wiretap Act and the Stored Communications Act for communications

11. *Id.*

12. *Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUST., BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#v5wwq [https://perma.cc/H9J8-6ZGT] (last visited Oct. 3, 2022).

13. *Id.*

14. *Id.*

15. 18 U.S.C.A. § 2511(1)(a) (West 2018).

16. 18 U.S.C.A. § 2510(4) (West 2002).

17. *See id.*

18. *See* 18 U.S.C.A. § 2701(a)(1)–(2) (West 2018).

19. Kerr, *supra* note 1, at 1212–13.

20. *See id.*

within the employment context.[21] Specifically, the ECPA permits an employer to monitor: (1) any employee communication related to a legitimate business purpose; (2) any communication consented to by an employee; and (3) emails and messages stored on an employer's network or server.[22] These are commonly referred to as the ECPA's business use exception, consent exception, and stored communications exception.[23]

1. The Business Use Exception

The business-use exception applies to the Wiretap Act, and it allows the interception and monitoring of any wire, oral, or electronic communication so long as the communication occurs "in the ordinary course of business."[24] Thus, even if an employee resisted the would-be illegal monitoring, an employer could continue such a practice if capable of showing that the monitoring was done "in the ordinary course of business."[25] In addressing the business use exception, courts have used two modes of analysis: content and context.[26] In the content analysis, courts examine the nature of the communication and generally allow an employer to monitor and intercept all business-related calls; however, employers can only monitor personal calls to the extent necessary to determine their nature.[27] In the context analysis, courts consider whether an employer had a legitimate business interest that justifies the interception and monitoring of employee calls.[28] For example, in *Arias v. Mutual Central Alarm Systems, Inc.*, the Second Circuit found an employer's eavesdropping on an employee's private conversation legal under the ECPA because the telephone conversation occurred in the ordinary course of business and the employer had legitimate business reasons for recording all telephone calls.[29]

---

21. Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 296 (2002).

22. Daniel Garrie & Yoav Griver, *Employer Best Practices for Monitoring Remote Devices*, LAW360 (Aug. 31, 2020, 12:44 PM), https://www.law360.com/articles/1305462/employer-best-practices-for-monitoring-remote-devices-?copied=1 [https://perma.cc/G5KC-CHYM].

23. Kesan, *supra* note 21, at 296.

24. Thomas Reuters Editorial Staff, *supra* note 2, at 5 (quoting U.S.C. § 2510(a)(i)).

25. *See id.*

26. Kesan, *supra* note 21, at 297–98.

27. *Id.* at 298.

28. *Id.*

29. *See* Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553, 559 (2d Cir. 2000).

2. The Consent Exception

The employee consent exception, like the business-use exception, applies to the Wiretap Act and allows an employer to intercept and monitor any communications where an employee has given "prior consent."[30] For example, in an action concerning an employee's claim of an invasion of privacy, courts consider whether the employee had a "reasonable expectation of privacy."[31] Generally, courts will find that an employee does not have a reasonable expectation of privacy in communications if the employee consents to the employer's monitoring practice, which often occurs through notice of the monitoring itself or the general availability of a policy.[32] Thus, even if an employee has a reasonable expectation of privacy, an employer could be released from liability through consent obtained explicitly or implicitly by the circumstances.[33] However, the ECPA does not define a "reasonable expectation of privacy," so inconsistent holdings often occur in the case-by-case approach courts use in considering invasion of privacy claims.[34] For example, in *Shefts v. Petrakis*, the court found that an employee did not have a reasonable expectation of privacy and had impliedly consented to monitoring because the employee had access to the company manual, which provided in writing that all communications were subject to monitoring.[35] However, the court in *Watkins v. L.M. Berry & Co.* found that an employee did not impliedly consent to monitoring simply because she accepted employment and had knowledge of the company manual, which described the employer's ability to monitor employees.[36]

3. The Stored Communications Exception

The stored communications exception, also referred to as the "provider exception," applies to the Stored Communications Act, and allows an employer to retrieve and monitor communications if the employer provides the service for such communications.[37] Similar to the consent exception, the language in the Act defining a "provider" is unclear.[38] A broad interpretation

30. Thomas Reuters Editorial Staff, *supra* note 2, at 6 (quoting U.S.C. § 2511(2)(d)).

31. Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELY TECH. L.J. 979, 981 (2011).

32. Determann, *supra* note 31, at 1005.

33. Kesan, *supra* note 21, at 296–97.

34. *See* Determann, *supra* note 31, at 1006.

35. *See* Shefts v. Petrakis, 758 F.Supp.2d 620, 634 (C.D. Ill. 2010).

36. Kesan, *supra* note 21, at 297 (discussing Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

37. *See* 18 U.S.C.A § 2701(c)(1) (West 2018).

38. Kesan, *supra* note 21, at 296.

would allow an employer to access and monitor any communication by or for an employee if they are sent or received through an employer's network.[39] By contrast, a narrow interpretation would not allow an employer who stores communications through a third-party, off-site carrier to access and monitor such communications.[40] For example, in *Fischer v. Mt. Olive Lutheran Church*, a Wisconsin court interpreted the stored communications exception narrowly and found that an employer who accessed an employee's emails via Hotmail, a web-based third-party server, would not be protected by the stored communications exception and would be subject to civil liability.[41]

III. THE MODERNIZATION OF THE WORKPLACE: WHERE WE CAME FROM AND WHERE WE ARE GOING

A. Advancements in Technology

Since the ECPA was enacted in 1986, technology in the United States has advanced significantly.[42] In the 1990s, the internet was born, which allowed people from all over the world to communicate instantaneously through the transmission of messages, emails, and eventually, video chat.[43] Then, in 2004, Facebook emerged as a platform to help friends stay connected, and quickly rose to become the world's largest social media platform.[44] Fast forward only three years later, and the iPhone was released, which forever changed the way people connect and communicate with one another.[45] Thus, while the ECPA's original intent was to protect electronic communications, the meaning and consideration of what constitutes electronic communication have changed drastically. Today, communications may include e-mail communications, texts stored on a company phone or computer, and, in some cases, posts made on social media websites accessible to employers.[46]

B. Changes in the Workplace

As technology has advanced, the workplace and employment environment have followed suit. Acting in the same manner as machines in the In-

39. *See id.*

40. *See id.*

41. Fischer v. Mt. Olive Lutheran Church, 207 F.Supp.2d 914, 926 (W.D. Wis. 2002).

42. *See* Kesan, *supra* note 21, at 304.

43. *See* Kevin Webb, *From the Internet to the iPhone, Here Are the 20 Most Important Inventions of the Last 30 Years*, BUS. INSIDER (May 17, 2019 5:17 PM), https://perma.cc/26KZ-CF4R].

44. *Id.*

45. *Id.*

46. *See* Determann & Sprague, *supra* note 31, at 1001–02.

dustrial Revolution, data analytics and algorithms have transformed the nature of labor and employment.[47] In recent years, employers have traded in office managers for high-functioning monitoring software, with promises of increased productivity and fundamental change.[48] While each software varies in its specific elements, most provide capabilities of monitoring keystroke logs, telephone usage, and the length of time between breaks.[49] Other software systems are capable of monitoring computer hard drives and searching for things that would be in violation of workplace policies, such as pornography, music, or movies.[50]

While monitoring software was already on the rise throughout the early 2000s, major events such as the COVID-19 shut downs drove the demand for employee surveillance software up by 58% in March of 2020.[51] In a study conducted by the Massachusetts Institute of Technology (MIT), researchers found that over one-third of U.S. employees began working from home after the pandemic struck; with the second most searched phrase in March 2020 being "how to monitor employees working from home," many employers sought help from various monitoring software services.[52] However, even after the threat of being exposed to COVID-19 has significantly subsided, many employees remain working from home; specifically, the Pew Research Center found that 61% of Americans with offices available still choose to work from home.[53]

As working from home has gained popularity among Americans, many have also requested "flexible work hours" from their employers and the ability to choose when to complete their assigned work, often outside of normal business hours.[54] Thus, unlike decades past when employees could rely on a

47. *See* Philip M. Nichols, *Bribing the Machine: Protecting the Integrity of Algorithms as the Revolution Begins*, 56 AM. BUS. L.J. 771, 772 (2019).

48. *See id.*

49. Gail Lasprogata, et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through A Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, 19 (2004).

50. *Id.* at 20.

51. *See* Simon Migliano & Christine O'Donnell, *Employee Surveillance Software Demand Up 58% Since Pandemic Started*, TOP10VPN (Aug. 8, 2022), https://www.top10vpn.com/research/covid-employee-surveillance/ [https://perma.cc/5YT9-9AG3].

52. *Id.*

53. Kim Parker et. al., *COVID-19 Pandemic Continues to Reshape Work in America*, PEW RSCH. CTR. 1, 4 (Feb. 16, 2022), https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/ [https://perma.cc/G5BN-MME4].

54. *See* Tapas K. Ray & Regina Pana-Cryan, *Work Flexibility and Work-Related Well-Being*, NAT'L LIBR. OF MED., 1-2 (2021).

typical nine-to-five workday, technology has now created a "boundary-less workplace" where employees can perform work outside of regular hours and from locations outside of the office.[55] As a result, such technology has created more opportunities to monitor employees in the office and at home.[56]

IV. IMPLICATIONS IN THE ABSENCE OF FEDERAL REGULATION

A. Vulnerability in Employees

In the absence of a federal regulation that covers the privacy rights of employees in terms of employee monitoring and surveillance, some states have enacted their own legislation, and others have remained silent.[57] Most recently, New York amended its Civil Rights Act to require any and all employers engaging in employee monitoring to notify employees with a written notice and obtain a written acknowledgment of the notice.[58] Similarly, Connecticut and Delaware have laws requiring employees subjected to employee surveillance to be notified of the company's monitoring practices and for such notice to remain in a conspicuous area in the workplace.[59] Colorado and Tennessee have adopted less stringent but effective statutes; at a minimum, they require employers to adopt policies regarding monitoring employee emails, which must remain visible and accessible by employees.[60]

In enacting such legislation, these states have minimized the discretion given to employers and their monitoring practices and have provided employees with the awareness and knowledge that their data may be accessible to their employers.[61] By contrast, other states, such as Texas, have remained silent, leaving the decision whether to notify employees of monitoring or enact company monitoring policies at all to employers' discretion.[62]

Without notice or access to an official policy, employees may lack knowledge or awareness of how their data is used and which of their communications are monitored.[63] While generally, courts believe that employees should not have a reasonable expectation of privacy for communications sent

55. Levison, *supra* note 3, at 469.

56. *Id.*

57. *See* Thomas Reuters Editorial Staff, *supra* note 2, at 15.

58. *See* Ali Jessani et. al., *New Rules and Risks in Employee Monitoring*, JD SUPRA (June 29, 2022), https://www.jdsupra.com/legalnews/new-rules-and-risks-in-employee-8336780/ [https://perma.cc/2KRE-RFBQ].

59. *Id.*

60. Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 294–98 (2011).

61. *C.f.* Determann & Sprague, *supra* note 31, at 1016.

62. *See* Jones, *supra* note 7, at 98.

63. Determann & Sprague, *supra* note 31, at 1018.

and received on a device owned by an employer, courts are also hesitant to believe that employees should have a reasonable expectation of privacy for personal uses on company computers.[64] Notably, the Supreme Court held that the inquiry into whether an employee has a reasonable expectation of privacy must be made on a case-by-case basis.[65]

However, the case-by-case approach adopted by the Supreme Court often leaves employees vulnerable and without clear expectations from their employers or the law. For example, the Court in *Stengart v. Loving Care Agency, Inc.* held that an employee did have a reasonable expectation of privacy for her communications even though they were sent on a work-issued computer because she was using her personal e-mail account and did not save the account's password on the computer.[66] By contrast, in *U.S. v. Hassoun*, the Court held that an employee should not have had a reasonable expectation of privacy for his communications because the e-mails at issue were sent on his work-issued computer and thus were subject to the monitoring practices of the employer.[67]

B. Counterproductivity for Employers

Employees are not alone in feeling the effects of monitoring practices; employers may also face consequences due to employee monitoring. While intended to boost efficiency, without regulation, monitoring efforts may prove to be counterproductive.[68] Specifically, rather than working harder, employees may be motivated to work less in an effort to "game the system."[69] In addition, as a result of feeling untrusted by an employer, an employee may begin to lose faith in their own capabilities and feel less confident.[70]

Further, inconsistent state regulations and contradictory rulings can leave employers defenseless to lawsuits for unintentionally violating state-specific monitoring practices.[71] Due to the case-by-case nature of determining whether an employee should reasonably expect privacy, an employer's monitoring practice may be legal today and illegal tomorrow.[72] For example, in *Vernars v. Young*, the court held that employees should have a reasonable

64. *Id.* at 1005.

65. Ciocchetti, *supra* note 60, at 300.

66. Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 321–22 (N. J. 2010).

67. U.S. v. Hassoun, No.04-60001-CR, 2007 WL 141151 at *2, 7 (S.D. Fla. Jan. 17, 2007).

68. Kesan, *supra* note 21, at 320.

69. *Id.*

70. *See id.*

71. Ciocchetti, *supra* note 60, at 347.

72. *See* Determann & Sprague, *supra* note 31, at 1018.

expectation that their personal, physical mail would not be opened or read by employers.[73] As follows, scholars raise the question of whether employees should have a reasonable expectation that their e-mails would not be opened or read.[74]

C. Amending the ECPA Through Federal Legislation

The Electronic Communications Privacy Act in its current state has left employees vulnerable to privacy rights violations and employers uncertain as to their duty to provide safeguards to their employees and the legal implications of monitoring employee activity.[75] However, by amending the ECPA, legislators could address current technological advancements, set guidelines for acceptable monitoring practices, and resolve the uncertainty surrounding employees' right to privacy.[76] Though some scholars advocate for the enactment of a new federal regulation specifically designated for employee monitoring procedures, an amended ECPA would likely effectuate many of the same goals as an entirely new federal statute.[77]

Specifically, in following the New York, Delaware, and Connecticut state legislatures, the ECPA could be amended to require employers to provide notice of their monitoring policies to employees.[78] In doing so, much of the ambiguity related to an employee's "reasonable expectation of privacy" would be resolved.[79] Rather than giving courts wide discretion in deciding whether an employee had actual or implied notice of a company's monitoring practice on a case-by-case basis, courts would decide cases more cohesively and predictably.[80]

In addition, like the New York state statute, the ECPA could benefit from an amendment that requires employees to acknowledge they received and understand a notice of a company's monitoring practice.[81] While it is already considered a best practice for employers to provide notice of company monitoring policies, without a specific requirement, notice can be provided simply by including the policy within the company handbook or by keeping the company policy in a place accessible to employees.[82] Problems sometimes arise when employees have access to employee monitoring prac-

73. Kesan, *supra* note 21, at 321.

74. *See id.*

75. *See* Levison, *supra* note 3, at 529.

76. *Id.*

77. *See id.*

78. *See* Determann, *supra* note 31, at 1018.

79. *See id.*

80. *See id.*

81. *See e.g.*, S. B. 2628, 2021 Leg., Reg. Sess. (N.Y. 2021) (enacted).

82. Determann, *supra* note 31, at 981.

tices but are unaware that they exist.[83] Thus, an acknowledgment from an employee showing that they understand the company may engage in monitoring will increase transparency and minimize the risk of litigation on the basis of invasion of employee privacy.[84]

V. CONCLUSION

Based on the preceding discussion, it is clear that as a result of technological advances and workplace changes, the Electronic Communications Privacy Act of 1986 has become outdated and ineffective in protecting employee privacy rights.[85] While the ECPA was enacted to address relative changes in technology, by failing to amend and adapt the ECPA, its goal has become void.[86] Further, states have been forced to address such technological advancements in their own statutes, which often leaves employees vulnerable and employers with significant discretion to monitor employee activity.[87] Until the ECPA addresses the interception and monitoring of communications on personal devices, social media accounts, or in employee homes, employees will often be left vulnerable, and employers with significant discretion to monitor employee activities.

83. *See id.*

84. *See* Senate Bill S628, THE NEW YORK STATE SENATE 1, 5, https://www.nysenate.gov/legislation/bills/2021/S2628?intent=support [https://perma.cc/NY5L-CJFR] (last visited Nov. 3 2022) (discussing the justification for S. B. 2628).

85. *See* Levison, *supra* note 3, at 471.

86. *See* Thomas Reuters Editorial Staff, *supra* note 2, at 1.

87. *See* Jones, *supra* note 7, at 99.