

2011

Workplace Privacy and Monitoring: The Quest for Balanced Interests

Ariana R. Levinson
University of Louisville

Follow this and additional works at: <https://engagedscholarship.csuohio.edu/clevstrev>



Part of the [Computer Law Commons](#), [Internet Law Commons](#), and the [Labor and Employment Law Commons](#)

[How does access to this work benefit you? Let us know!](#)

Recommended Citation

Ariana R. Levinson, *Workplace Privacy and Monitoring: The Quest for Balanced Interests*, 59 Clev. St. L. Rev. 377 (2011)
available at <https://engagedscholarship.csuohio.edu/clevstrev/vol59/iss3/6>

This Article is brought to you for free and open access by the Journals at EngagedScholarship@CSU. It has been accepted for inclusion in Cleveland State Law Review by an authorized editor of EngagedScholarship@CSU. For more information, please contact library.es@csuohio.edu.

WORKPLACE PRIVACY AND MONITORING: THE QUEST FOR BALANCED INTERESTS

ARIANA R. LEVINSON*

I. INTRODUCTION	377
II. ELECTRONIC COMMUNICATIONS PRIVACY ACT.....	380
A. <i>Wiretap Act</i>	381
1. Interception.....	381
2. Exceptions	384
B. <i>Stored Communications Act</i>	386
1. Electronic Storage	386
2. Exceptions	388
III. STATE LAWS.....	390
IV. TORT INVASION OF PRIVACY	392
V. FOURTH AMENDMENT	395
VI. CONCLUSION	396

I. INTRODUCTION

We all are aware at this point that we have rapidly advancing technology. It's advancing faster than it has in previous times, and this creates what Kathy Stone at the UCLA School of Law has termed the "boundary-less workplace."¹ So we have employees who are working at home and can easily take their offices home with them. What this also means is that we have employees who are doing all kinds of personal tasks, beyond what they could have done in previous years, in the workplace.

*Assistant Professor, University of Louisville, Louis D. Brandeis School of Law; J.D., University of Michigan Law School. This article is a transcript, with minor changes to ensure readability, several asides deleted, and additions to the Conclusion, of The Littler Mendelson Employment and Labor Law Lecture at Cleveland-Marshall College of Law presented on March 31, 2011. The author thanks Candice Hoke the title and the opportunity to lecture, Daniel Myers, 2010-2011 Submissions Editor for the *Cleveland State Law Review* for transcribing the lecture and Elisabeth Fitzpatrick for her superb research and editorial assistance.

¹ Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1037 n.8 (2006).

For employers this raises a number of concerns.² First, employees may be spending an inordinate amount of time doing personal tasks in the workplace.³ Second, some of the tasks they may be doing might be inappropriate for the workplace. They may be looking at child pornography,⁴ or they may be engaging in messaging that can be considered sexual harassment.⁵ Finally, it is very easy, at the push of a button, to put information out to the public. This might happen inadvertently or purposely. Those who predominantly represent employers can probably think of some other difficulties that advancing technology is creating.

Now, on the flip side, we have some concerns from the employees' perspective. The employers have a much greater ability to monitor employees because of the advancing technology⁶—the technology is a lot more sophisticated than it used to be. So there is a greater risk that employers either purposely or inadvertently are discovering personal information about employees. There have also been some psychological studies that show when monitoring is engaged in certain ways it can cause employees high levels of stress or even physical discomfort.⁷ Those of you who predominantly represent either employees or unions can probably think of some other difficulties that your clients are encountering due to this advancing technology.

In terms of the statistics, there are a number of different studies, but perhaps the best one is from the AMA, the American Management Association, because it has done this three times.⁸ The AMA has collected data that is self reported, and it tends to be larger companies.⁹ Maybe smaller companies don't exactly follow this pattern, but our best estimate is that they are close, so these look like fairly good statistics. We can see in 2001 that 77 percent of employers were engaged in monitoring.¹⁰ This may have increased slightly or decreased slightly, but whatever has happened, we know that this is a significant amount of employers—much greater than a majority—that are engaging in monitoring of their employees. We can also

² See Ariana R. Levinson, *What Hath the Twenty First Century Wrought? Issues in the Workplace Arising from New Technologies and How Arbitrators Are Dealing with Them*, 11 *TRANSACTIONS: TENN. J. OF BUS. L.* 9 (2010).

³ *Id.* at 16-17.

⁴ *Id.* at 19.

⁵ *Id.* at 19-23.

⁶ *Id.* at 9.

⁷ Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 *J. MARSHALL L. REV.* 139, 144 (1994).

⁸ 2007 *Electronic Monitoring & Surveillance Survey* 6, 10 (2008), AMA/EPOLICY INST. RESEARCH, AM. MGMT. ASS'N, <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf>; Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 *COMP. LAB. L. & POL'Y J.* 471, 474 (2002).

⁹ Finkin, *supra* note 8, at 474.

¹⁰ *Id.*

see the great rise in monitoring of computers and electronic files in a ten-year period between 1997 and 2007.¹¹

Finally, we can see some of the newer technologies. In 2007, twelve percent of the reporting employers were monitoring the blogosphere, eight percent were monitoring GPS vehicle tracking, and ten percent were monitoring social networking sites.¹² Probably, some of you are working with social networking policies with the companies that you are involved with. This is a hot topic right now. Hopefully the AMA will do this study again within the next couple years, and we will see whether the numbers on monitoring blogs and social networking sites have increased.

In terms of the technology itself—which I am not a technology expert, I read about it and talk to the wonderful IT people that work in my building—there is something called a “key logger,” or it is referred to sometimes as a key catcher.¹³ It can either be hardware—it is just that little round thing that hooks where your keyboard hooks into your computer¹⁴—or it can be software. If it is software, it creates a printout. It logs every keystroke that the employee is making, so the employers can use this to capture the keystrokes that their employees are making and have a record of that.¹⁵

Another type of software sold by one company has come up in several of the cases that have been litigated. This company is called SpectorSoft, and it has a number of different softwares, but one of its software programs captures everything that appears on the computer screen.¹⁶ The co-founder of the company made the following statements about the software program: “[the program] is designed to make it easier for parents to monitor their children’s Internet use and for employers to monitor their employees’ Internet use.”¹⁷ The software “virtually” contemporaneously captures “all instant messages, sent and received e-mails, web searches, online chats, file transfers, electronic data and other activity from the computer”¹⁸ It is specifically designed for employers to monitor their employees’ Internet use, and it captures this information contemporaneously.

That gives you a picture of what the technology looks like, what the statistics are, and what we are grappling with in terms of the law here. In terms of the law, I am going to talk about the Electronic Communications Privacy Act (“ECPA”).¹⁹ There

¹¹ Compare 2007 *Electronic Monitoring & Surveillance Survey*, *supra* note 8 (reporting 43% of employers monitor computer files and e-mail), with Finkin, *supra* note 8, at 474 (reporting 13.7% of employers monitor computer files and 14.9% monitor e-mail).

¹² 2007 *Electronic Monitoring & Surveillance Survey*, *supra* note 8.

¹³ SEARCHMIDMARKETSECURITY.COM, *Definition of Keylogger (Keystroke Logger, Key Logger, or System Monitor)*, <http://searchmidmarketsecurity.techtarget.com/definition/keylogger> (last updated May 2004).

¹⁴ SEARCHMIDMARKETSECURITY.COM, *supra* note 13.

¹⁵ *Id.*

¹⁶ *Hayes v. Sectorsoft Corp.*, No. 1:08-CV-187, 2009 U.S. Dist. LEXIS 102637, at *7 (E.D. Tenn. Nov. 3, 2009).

¹⁷ *Id.* at *6.

¹⁸ *Id.* at *3.

¹⁹ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

are also some state statutes that are going to be relevant. There is the tort that we are all very familiar with, dating back to Brandeis' day, of the invasion of privacy, which is invasion of seclusion.²⁰ And then finally we know that right now there is the hot topic with the *Quon* case coming down last term with the Fourth Amendment and public-sector employers and employees.²¹

Before I jump into the law, try to think about an employer's perspective and an employee's perspective on these issues. Even if you don't predominantly represent employers or employees, you are probably an employee or, perhaps, an employer yourself; maybe you work for a company. So, everybody has perspective on these issues.

If you are thinking about this from the employer's perspective as you are thinking about this law, try and ask yourself some questions: Is there some sort of safe harbor here? If the employer is trying to protect employees' privacy and also meet the necessary needs to make sure that the company is running lawfully and efficiently, is there some type of policy or action that the employer can take to be protected legally? Is there any uniformity here? Is it such that the employer knows what it should do and whether it can do this in all jurisdictions, or does the employer have to grapple with different laws and different jurisdictions? You can ask yourself: is this overly technical? Is it difficult to understand? Is an employer going to have to go out and hire an attorney to be able to grapple with these laws?

From the employee's perspective, you can ask yourself: is there some type of minimal level of protection for privacy here? Is there any baseline protection for employees' privacy in the workplace? Is this clear for employees? Can they tell that they may be doing something that the employer should or could investigate, or when they are doing something that the employer shouldn't or couldn't investigate? And finally, is there any remedy if an employee feels that privacy has been invaded?

II. ELECTRONIC COMMUNICATIONS PRIVACY ACT

First, we have the ECPA.²² A lot of the courts and the scholars have indicated that it is very technical, difficult to interpret, and one of the most difficult acts out there.²³ Having spent the last year and a half looking at it, I throw my weight behind this sentiment. It is very technical and I'm going to give you a simplified view—I'm just going to give you the nutshell view so you can have some baseline understanding of what's involved with the ECPA.

²⁰ See, e.g., *Melvin v. Reid*, 297 P. 91 (Cal. Dist. Ct. App. 1931); *Rhodes v. Graham*, 37 S.W.2d 46 (Ky. Ct. App. 1931); *White v. Safe Deposit & Trust Co. of Balt.* 118 A. 77 (Md. 1922); *Judevine v. Benzies-Montanye Fuel & Warehouse Co.*, 269 N.W. 295 (Wis. 1936).

²¹ *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

²² Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

²³ *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994); Connie Barba, *'That's No 'Beep', That's My Boss: Congress Seeks to Disconnect the Secrecy of Telephone Monitoring in the Workplace*, 21 J. MARSHALL L. REV. 881, 883 n.17 (1988); Jeremy E. Gruber & Lewis Maltby, *The Need for Reasonable Policies*, [213-FEB.] N.J. LAW. 41, 43 (2002); 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, 1208 (2004); Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 130 (2005).

The ECPA has three titles.²⁴ We are curious about two of the titles because they relate to when employers monitor their employees' electronic communications. Title I is commonly known as the Wiretap Act.²⁵ If there is anyone with criminal-law experience, you may have come across the ECPA in that context. The Wiretap Act prohibits the intentional acquisition of the contents of electronic communications, which is the interception of electronic communications.²⁶ The Stored Communications Act, Title II, prohibits the intentional unauthorized access to stored communications.²⁷ So we have one title, on the one hand, that is dealing with interception and the other one is dealing with stored communications. The distinction matters because the Wiretap Act is considered to be more restrictive in terms of what employers and others can do when they are monitoring.²⁸ Also, in certain circuits like the Fourth Circuit, the damages are more limited under the Stored Communications Act,²⁹ so again the Wiretap Act is considered to provide broader protections to employees. And then finally there are some disclosure provisions in the Wiretap Act³⁰ that I am not going to go into, but for that reason it could also be considered more protective of employee privacy.

A. Wiretap Act

So we start with the Wiretap Act, and you will see all these issues listed out in front of you,³¹ all of them open issues, and for both of these Acts we will have court cases on every open issue that reach opposite results, sometimes diametrically opposed results, on very similar facts. I will not go into all of them, but I will provide some examples.

1. Interception

The first thing that comes up with the Wiretap Act is what is "interception." At the time that the ECPA was passed, it was the 1980s and the technology looked very different at that time. If you were intercepting a wire communication, you got it in transit—it was not stored, and it was being passed from the sender to the receiver. When you flash forward to today, you have all kinds of electronic communications like email and text messages that pass from sender to receiver in under a second.

²⁴ Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

²⁵ Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1946 (2009).

²⁶ Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 39 (2011).

²⁷ Gleicher, *supra* note 25.

²⁸ Robert A. Pikowsky, *Privilege and Confidentiality of Attorney-Client Communication Via Email*, 51 BAYLOR L. REV. 483, 553 (1999).

²⁹ Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 207 (4th Cir. 2009).

³⁰ 18 U.S.C. § 2511(1)(b)-(d) (2006 & Supp. 2008).

³¹ *See id.* The issues are (1) interception; (2) consent; (3) provider; (4) ordinary course of business; and, (5) interstate commerce.

And during most of the time that they are passing from sender to receiver, they are stored. They are not un-stored and in transit, but stored and in transit.³²

So the issues are: does “interception” include acquiring stored communications? And does the communication need to be in transit? From the earliest cases, what the courts said was that it needs to be in transit and that it cannot be stored.³³ For instance, we have the *Bohach*³⁴ case. What happened in this case was that there was a paging system, and an employee could send text messages through the paging system.³⁵ The employee could do this in one of three ways:³⁶ through the actual paging device; over a telephone line; or on the employer’s computer.³⁷ The case arose because of messages that were sent on the employer’s computer.³⁸ The employee would type the message onto the employer’s computer. It would then go off to the paging company. The paging company would send it on to the recipient.³⁹ The employer was engaging in an internal investigation and decided to read the employees’ messages that were logged on the computer.⁴⁰ So the question was whether these messages were “intercepted” when the computer acquired and stored them.⁴¹ The court said no.⁴² The court reasoned it was not an interception because the employer was dealing with stored communications, and a stored communication cannot be intercepted.⁴³ It is not like a hidden microphone picking up what we are conversing about.⁴⁴ It is not like a wiretap on a phone line; it is stored communication. That was the traditional view.

More recently courts have been more willing to recognize that the technology involves storing information while it is in transit. They are willing to recognize that information can be stored and still intercepted. They still, however, want it to be during transmission to constitute an interception. In *Global Policy Partners*, a 2009 case,⁴⁵ for instance, there was a husband and wife team—these cases all make for interesting facts—and they were working in a company, and then they decided to

³² *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 886-87 (9th Cir. 2002) (Reinhardt, J., dissenting).

³³ *See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996).

³⁴ *Bohach*, 932 F. Supp. at 1232.

³⁵ *Id.* at 1233-34.

³⁶ *Id.* at 1234.

³⁷ *Id.*

³⁸ *Id.* at 1233.

³⁹ *Id.* at 1234.

⁴⁰ *Id.* at 1233.

⁴¹ *Id.* at 1236.

⁴² *Id.*

⁴³ *Id.* 1236-37.

⁴⁴ *Id.* at 1236.

⁴⁵ *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009).

separate and divorce.⁴⁶ The husband obtained the password to the wife's email communications, and, in particular, he went into her business email account and read all of the messages her divorce attorney had sent to her.⁴⁷ The first question that arises, if she wants to sue under the Wiretap Act, which she does, is whether this is an "interception."⁴⁸ This is what the court tells us—we have a football analogy:

Thus, interception includes accessing messages in transient storage on a server during the course of transmission, but does *not* include accessing the messages stored on a destination server. In other words, these statutes give "intercept" its common meaning, which is perhaps best understood through a football analogy. In American football, a ball can only be intercepted when it is "in flight." Once a pass receiver on the offensive team has caught the ball, the window for interception has closed, and defenders can only hope to force a fumble. In essentially the same way, a qualifying "intercept" under the ECPA . . . can only occur where an e-mail communication is accessed at some point between the time the communication is sent and the time it is received by the destination server . . .⁴⁹

Notice the court says this has reached the destination server, regardless of whether she read the messages or not, and some of them she has not read, so she had not received.⁵⁰ This will not constitute an intercept.⁵¹

Then we have the third approach, which is that taken in *Shefts*,⁵² and this approach is the one that the federal district courts in Illinois and the Seventh Circuit courts are using. What happens in *Shefts* is there is an employee, and he is using a Blackberry, and allegedly he is sexually harassing other employees and breaching his fiduciary duties.⁵³ The employer decides that it needs to investigate whether these allegations are true. One of the ways that it investigates is it has IT convert the software on the computer so that all of the suspected employee's text messages on his Blackberry are captured onto the computer.⁵⁴ So the first issue is, when the computer captures those text messages, is it intercepting them when it acquires the messages? The *Shefts* court says yes.⁵⁵ The court reasons that it is an interception when the computer acquires those messages.⁵⁶ So we have three different approaches to this question of what constitutes an "interception."

⁴⁶ *Id.* at 633.

⁴⁷ *Id.* at 634.

⁴⁸ *Id.* at 637.

⁴⁹ *Id.* at 638 (citations omitted).

⁵⁰ *Id.* at 639.

⁵¹ *Id.*

⁵² *Shefts v. Petrakis*, 758 F. Supp. 2d 620 (C.D. Ill. 2010).

⁵³ *Id.* at 625.

⁵⁴ *Id.* at 625-26.

⁵⁵ *Id.* at 630.

⁵⁶ *Id.*

2. Exceptions

Once you have an interception—you have determined an employer has intercepted somebody's electronic communications—you check whether the employer fits into any of the exceptions, and remember there are three. They are consent, ordinary course of business, and provider.⁵⁷ In terms of consent, there are a lot of cases from telephone issues and pre-electronic communication, which provide a long history of what consent means.⁵⁸ It is very explicit in the legislative history that this is implied-in-fact consent. You have to look at the facts,⁵⁹ consider the totality of the circumstances, and determine if the person knew he or she was being monitored and whether the person assented. The person doesn't actually have to say "I consent to you monitoring," but the person needs to know the person is being monitored and go ahead and engage in the conduct in the face of that knowledge.⁶⁰ Consent is important because it is what encourages employers to have policies. Policies encourage deliberate thinking on the part of employers and give employees the opportunity to change their behavior.⁶¹ That makes the consent exception an important one.

The ordinary course of business exception is a little trickier. It only applies when you are using telephone and telegraph equipment generally.⁶² The Second Circuit has ruled otherwise though.⁶³ It applies it to electronic communications regardless of whether there is telephone or telegraph equipment involved.⁶⁴ But if you fall into the circumstance like a Blackberry or a cell phone that is telephone equipment and contains electronic communications, then there are further requirements. These cases are all over the map. In some jurisdictions, if you have a legitimate business reason and you are an employer, then you are acting in the ordinary course of business.⁶⁵ In other jurisdictions, you need not only a legitimate business reason, but it needs to be a routine practice—a practice that the business ordinarily engages in.⁶⁶ The Sixth Circuit requires a legitimate business reason, that it be in the ordinary

⁵⁷ Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. (forthcoming 2011).

⁵⁸ See, e.g., *United States v. Townsend*, 987 F.2d 927 (2d Cir. 1993); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992); *United States v. Splawn*, 982 F.2d 414 (10th Cir. 1992); *United States v. Carrazana*, 921 F.2d 1557 (11th Cir. 1991); *Shubert v. Metrophone, Inc.*, 898 F.2d 401 (3d Cir. 1990).

⁵⁹ Levinson, *supra* note 57, at 34.

⁶⁰ See *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003); *Adams v. City of Battle Creek*, 250 F.3d 980, 992 (6th Cir. 2001); *Potter v. Havlicek*, No. 3:06-CV-211, 2007 WL 539534, at *8 (S.D. Ohio 2007).

⁶¹ Levinson, *supra* note 57, at 34.

⁶² *Id.* at 38.

⁶³ *Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 504 (2d Cir. 2005).

⁶⁴ *Id.*

⁶⁵ *Arias v. Mutual Cent. Alarm Servs., Inc.*, 182 F.R.D. 407, 416 (S.D.N.Y. 1998).

⁶⁶ *Briggs v. Am. Filter Co.*, 630 F.2d 414, 420 (5th Cir. 1980).

course of things, a routine practice, and notice.⁶⁷ So that circuit is the most stringently restrictive in terms of the ordinary course of business exception.

The courts are also all over the map on if an employer is listening to personal conversations, or in this context knows that an electronic communication is personal, it should stop monitoring at that point. There are some courts that don't care; if you have a legitimate business reason, you can monitor personal information.⁶⁸ Others say you should stop monitoring when you hear "hi, honey" on the telephone.⁶⁹

The third exception is the provider exception.

It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of rights or property of the provider of that service . . .⁷⁰

Just looking at the face of this exception, what does it require? It requires some type of agent of the provider; it requires that the agent be engaged in the ordinary course of employment; it requires that the agent be acting as a necessary incident to protect the rights or property of the provider, or because the agent is an IT person, and it is part of the job requirements.⁷¹ So we have courts that have interpreted this more or less broadly.

Specifically, this language, "rights or property" of the employer, has been interpreted more or less broadly. There is the *Kinesis* case, which comes from North Carolina.⁷² In this case, there was an employee who left and had breached, or allegedly breached, a covenant not to compete.⁷³ When the employee left, the employer went back through the business email of that employee to look for evidence of the breach of the covenant not to compete.⁷⁴ The court said "yes," that is protection of the employer's rights and property.⁷⁵ So, that employer acted lawfully and did not violate the Wiretap Act.⁷⁶

And then with an even broader interpretation of this language, we have *Freedom Calls*.⁷⁷ Here, the employee was terminated, and the employer went back again into

⁶⁷ *Adams v. Battle Creek*, 250 F.3d 980, 984 (6th Cir. 2001).

⁶⁸ *Amati v. Woodstock*, 176 F.3d 952, 956 (7th Cir. 1999).

⁶⁹ *See Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 583 (11th Cir. 1983).

⁷⁰ 18 U.S.C. § 2511(2)(a)(i) (2006 & Supp. 2008).

⁷¹ *Id.*

⁷² *Kinesis Adver., Inc. v. Hill*, 652 S.E.2d 284 (N.C. Ct. App. 2007).

⁷³ *Id.* at 289.

⁷⁴ *Id.* at 296.

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Freedom Calls Found. v. Bukstel*, No. 05CV5460(SJ)(VVP), 2006 WL 845509, at *27 (E.D.N.Y. Mar. 3, 2006).

the business email and responded to the messages that were coming in using the employee's email account on the employer's business email.⁷⁸ The court here took an even broader approach. The court said "yes," the employer was the provider.⁷⁹ The court reasoned that the employer needed to timely respond to messages and needed to make sure that the business acted efficiently, so this falls within the protection of the rights or property of the employer.⁸⁰

But there is an interesting California case, *O'Grady*,⁸¹ and it is not about this provider exception but a provider exception with exactly the same language in the Stored Communications Act, and it applies to the disclosure provisions there.⁸² But what is interesting is that the court drew a very firm line saying that "rights or property" does not mean any cost to the employer.⁸³ This needs to be somehow restricted to rights and property that relate to the employer's responsibility as a service provider because most employers are not service providers.⁸⁴ They act as service providers, but they also have some other primary business that they are engaged in. So you see those cases interpreting the language of the provider exception come out differently,

That is the Wiretap Act. You want to ask yourself whether it is an interception, and, if so, whether the employer falls within one of the exceptions.

B. Stored Communications Act

Then we get to the Stored Communications Act.⁸⁵ It is exactly the same—it is really complicated; it has all these issues (you can see them listed⁸⁶); and the courts have gone every which way again on all of them.

1. Electronic Storage

The first question we encounter here is: what is a stored communication? The Act prohibits unauthorized access to stored communications.⁸⁷ This is the definition of electronic storage:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B)

⁷⁸ *Id.* at *3.

⁷⁹ *Id.* at *27.

⁸⁰ *Id.*

⁸¹ *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72 (Ct. App. 2006).

⁸² *Id.* at 83-87.

⁸³ *Id.* at 85.

⁸⁴ Levinson, *supra* note 57, at 37.

⁸⁵ 18 U.S.C. §§ 2701-2712 (2006 & Supp. 2008).

⁸⁶ *See id.* The issues are: (1) electronic storage; (2) without authorization; (3) obtains, alters, prevents authorized access; (4) provider exemption, and; (5) user authorization.

⁸⁷ 18 U.S.C. § 2701 (2006 & Supp. 2008).

any storage of such communication by an electronic communication service for purposes of backup protection of such communication.⁸⁸

Most courts have said this is very broad.⁸⁹ If an ISP provider has the electronic communication, it is a stored communication. But not all of them.

One good example of a court interpreting the language broadly is the *Fischer* case.⁹⁰ In this case, a church was the employer of a youth pastor.⁹¹ The youth pastor's obligations were to counsel youth but also periodically adults.⁹² Somebody thought that they overheard a sexual conversation between the youth pastor and another male adult.⁹³ The employer was concerned about this and decided to investigate. The employer hired an expert.⁹⁴ The expert went onto the work computer and guessed at what the Hotmail account password of the employee was.⁹⁵ The employee had apparently not been using the Hotmail account to work and had not established the account at work, and it was a private, personal account.⁹⁶ The employer went into the account, read the messages, and printed some of them out.⁹⁷ The first question is: were those stored communications? The court said yes.⁹⁸ The court reasoned the messages were there on the hotmail server, they were stored there, and that was a stored communication.⁹⁹

But there are other courts, and these are in the minority, which have said "no," the term "electronic storage" is not that broad. In particular, there is an interesting case—the *Flagg* decision.¹⁰⁰ The *Flagg* decision is out of the Eastern District of Michigan, and it has complicated facts. What it boils down to is whether messages created by employees of a city were in electronic storage.¹⁰¹ The city had a text messaging service, and it stopped using it.¹⁰² But the service continued to retain copies of those messages.¹⁰³ The question was: were those stored? The court said

⁸⁸ 18 U.S.C. § 2510(17) (2006 & Supp. 2008).

⁸⁹ Levinson, *supra* note 57, at 51.

⁹⁰ *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914 (W.D. Wis. 2002).

⁹¹ *Id.* at 917.

⁹² *Id.*

⁹³ *Id.* at 918.

⁹⁴ *Id.* at 920.

⁹⁵ *Id.*

⁹⁶ *Id.* at 917.

⁹⁷ *Id.* at 920.

⁹⁸ *Id.* at 925-26.

⁹⁹ *Id.* at 925.

¹⁰⁰ *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008).

¹⁰¹ *Id.* at 359.

¹⁰² *Id.* at 347-48.

¹⁰³ *Id.* at 348.

no.¹⁰⁴ The court reasoned that the copy retained by the service was the only copy, and that the only copy cannot be a backup copy.¹⁰⁵ So the court held the messages were not stored. And you will see other cases going both ways.¹⁰⁶

2. Exceptions

There are two exceptions. We are not going to go into “Without Authorization.” It has a lot of case law.¹⁰⁷ Assuming the electronic communication is stored, and you accessed it without authorization, then you come to two exceptions—the provider exception and the user exception. They are both authorization exceptions.

The provider exception looks like this: “Subsection (a) of this section does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service.”¹⁰⁸ Notice how much more broad it is than the provider exception seen in the Wiretap Act. Almost anytime an employer is providing the electronic communication service, and it is stored communications, the employer will be able to access them under this provider exception.¹⁰⁹ Now, if it is a third-party provider then that is different, like with the text messaging companies.¹¹⁰ That gets into the distinction between electronic communications services and remote computing services. Those won’t be discussed, but that distinction determines, when dealing with a third-party provider, whether the third-party provider can release the electronic communication to the employer or not.¹¹¹

The exception that has some interesting cases is the “user authorization” exception. It is interesting because you have, under the Stored Communications Act, a very broad provider exception, but the user exception is perhaps the exception that has been most restrictively interpreted by the courts. So it is very hard then to

¹⁰⁴ *Id.* at 363.

¹⁰⁵ *Id.* at 362-63.

¹⁰⁶ *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (holding the messages were stored); *KLA-Tencor Corp. v. Murphy*, 717 F. Supp. 2d 895, 904–05 (N.D. Cal. 2010) (assuming without deciding that message was not stored); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (holding the messages were stored); *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (holding the messages were stored).

¹⁰⁷ *See, e.g.*, the following cases discussing authorization, *Monson v. Whitby Sch., Inc.*, No. 3:09CV1096(MRK), 2010 WL 3023873, at *5 (D. Conn. Aug. 2, 2010); *Global Policy Partners v. Yessin*, 686 F. Supp. 2d 631, 636 (E.D. Va. 2009); *Pure Power Boot Camp*, 587 F. Supp. 2d at 562; *Cardinal Health 414, Inc.*, 582 F. Supp. 2d at 976; *Wyatt Tech. Corp. v. Smithson*, No. C05-1309DT(RZx), 2006 WL 5668246, at *9 (C.D. Cal. Aug. 14, 2006) *aff’d in relevant part*, 345 Fed. Appx. 236 (9th Cir. 2009); *Borninski v. Williamson*, No. Civ.A.3:02CV1014-L, 2005 WL 1206872, at *12 (N.D. Tex. May 17, 2005); *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000).

¹⁰⁸ 18 U.S.C. § 2701(c)(1) (2006 & Supp. 2008).

¹⁰⁹ *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2004); *Freedom Calls Found. v. Bukstel*, No. 05CV5460(SJ)(VVP), 2006 WL 845509, at *27 (E.D.N.Y. Mar. 3, 2006).

¹¹⁰ Levinson, *supra* note 57, at 52, 56.

¹¹¹ *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008).

get user authorization. One interesting case is *Pure Power Boot Camp*.¹¹² This employee did something we should never do. He left this company and set up a competing fitness center, but on the employee's old work computer, he had accessed his Hotmail and Gmail accounts.¹¹³ When he accessed his Hotmail account, he used the "remember my password" function.¹¹⁴ Don't use that function. He left the password there on his employer's computer. And when he left and established his new business, the employer went right on there, got the password, and went right into his personal email account.¹¹⁵ The employer had a policy, and this is what the policy said: "[E]-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system. This includes the use of personal e-mail accounts on Company equipment."¹¹⁶ It looks pretty broad, right? You would think that it authorized the employer to go on and get the password that the employee inadvertently stored on the employer's computer. But the court said "no," this was not authorized by the user.¹¹⁷ The analogy that the court used was if the user leaves a key at the front desk to the user's house, with the receptionist, does that authorize the management to take the key, go to the house, and rummage through the employee's belongings?¹¹⁸ The court reasoned that even in the face of this policy, that is not user authorization.¹¹⁹

The other issue that comes up in these user authorization cases is illustrated by *Pietrylo*.¹²⁰ What happened here is that employees were using a chat group.¹²¹ The case does not reflect what was on there, but I imagine it was disparaging of the employer. They were using the chat group, and one of the managers asked one of the employees to give the password to the manager, and the employee did.¹²² But the court found that was not user authorization because the employee felt pressured to give the manager the password.¹²³ The employee felt that if she hadn't given it to the manager, there would have been negative consequences.¹²⁴ So again, that was not found to be user authorization.

That is the ECPA in a nutshell. Try to simplify it, and think about how understandable these laws are.

¹¹² *Pure Power Boot Camp*, 587 F. Supp. 2d at 548.

¹¹³ *Id.* at 552.

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 561-62.

¹¹⁸ *Id.* at 561.

¹¹⁹ *Id.* at 562.

¹²⁰ *Pietrylo v. Hillstone Rest. Group*, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

¹²¹ *Id.* at *1.

¹²² *Id.* at *1, *3.

¹²³ *Id.*

¹²⁴ *Id.*

III. STATE LAWS

Once you have tried to figure out your rights as an employer or as an employee under the ECPA, then you need to look at your specific state law. Most states have some kind of mini-ECPA, and in some of them there is a two-party consent requirement, so it is not enough that one party consents. I looked up Ohio, and it does not seem to have two-party consent, which is like the ECPA.¹²⁵ But there are other states that have different kinds of provisions that will come into play here, so employers need to be aware of them, as do employees in these particular states.

Many states have minimum privacy levels: New York and Rhode Island are just examples. These are laws that protect employees' privacy in places, like restrooms, that most of us can agree that employees would be entitled to some type of privacy in. They differ by state, so you can see New York prohibits two-way mirrors, video in the restroom, and video in the locker and changing rooms.¹²⁶ Whereas Rhode Island just prohibits video or audio in the restroom.¹²⁷

There are also a couple of states, Connecticut¹²⁸ and Delaware,¹²⁹ that have notice laws. These are modeled on the NEMA—Notice of Electronic Monitoring Act—that failed to pass around 2000.¹³⁰ It was a proposed federal statute. These are based on that same concept, most likely,¹³¹ that employers are more reflective when they need to provide notice. They think more about how to monitor. And employees have the opportunity to change their behavior. There are differences again between the two states. The Connecticut statute is really broad. You need to give notice of any kind of monitoring that is not direct observation.¹³² The Delaware statute is more limited. It covers monitoring of telephone, internet, and email.¹³³ Connecticut requires written notice.¹³⁴ In Delaware, it is okay to have something that pops up on the screen when the employee logs in as the form of notice that is provided.¹³⁵ Connecticut has a labor commissioner proceeding.¹³⁶ In Delaware, you file individual suit.¹³⁷ So as you are thinking about ideally what would work here,

¹²⁵ OHIO REV. CODE ANN. § 2933.52 (West, Westlaw through 2011 Files 1 - 19, of the 129th GA (2011-2012)).

¹²⁶ N.Y. LAB. LAW § 203-c (McKinney 2006).

¹²⁷ R.I. GEN LAWS ANN. § 28-6.12-1 (West, Westlaw through chapter 321 of the January 2010 session).

¹²⁸ CONN. GEN. STAT. § 31-48d (2008).

¹²⁹ DEL. CODE ANN. tit. 19, § 705 (2008).

¹³⁰ Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000).

¹³¹ *See id.* The Acts do not explicitly state the concept on which they are based.

¹³² § 31-48d.

¹³³ tit. 19, § 705.

¹³⁴ § 31-48d.

¹³⁵ tit. 19, § 705.

¹³⁶ § 31-48d.

¹³⁷ tit. 19, § 705.

these state statutes are a good laboratory for looking at what would be a good balance of employers' and employees' interests.

In Michigan and in Illinois, there are acts that govern the integrity of personnel records.¹³⁸ Again these are not specifically geared towards electronic monitoring, but what they prohibit is gathering information about people's non-employment related communication.¹³⁹ And of course if the employee authorizes this, it is all right in both of these states, but, in that instance, an employer would need to have a record of what was gathered, and the employee has a right to review the information.¹⁴⁰ So there are differences again. There are exemptions for when an employee is engaging in criminal activity, and the notice that has to be given in Michigan in that situation is different than in Illinois, where you only give notice if you take adverse action based on the criminal investigation.¹⁴¹ Michigan has a lawsuit; Illinois has the Department of Labor.¹⁴² Illinois includes anti-retaliation provisions and provisions that give union representatives the right to review information.¹⁴³

These are interesting statutes—lawful off-duty activity statutes. Several scholars have written about them.¹⁴⁴ You may have heard them referred to as lifestyle discrimination statutes. The goal of these statutes is that if an employee is engaging in lawful conduct off duty, then they should not suffer adverse consequences at work. Again, though, there are differences between the coverage of them. In North Dakota and New York, the prohibition is pretty broad—any type of adverse action.¹⁴⁵ In Colorado, it is just prohibiting termination because of lawful off-duty conduct.¹⁴⁶ In North Dakota, the coverage is broad; it is any type of lawful off-duty conduct.¹⁴⁷ In New York, it is very restrictive, so the category that applies here is recreational activities. If you are on Facebook, blogging, in a chat room, or engaged in some sort of recreational activity, it might fall within the protections of the New York statute. The exceptions in the enforcement provisions vary.

¹³⁸ MICH. COMP. LAWS ANN. § 423.508 (West, Westlaw through P.A. 2011, No.64 (except 62), of the 2011 Regular Session, 96th Legislature); 820 ILL. COMP. STAT. ANN. 40/9 (West, Westlaw through P.A. 97-13, with the exception of P.A. 97-6, of the 2011 Reg. Sess.).

¹³⁹ § 423.508 (Westlaw); 40/9 (Westlaw).

¹⁴⁰ § 423.508 (Westlaw); 40/9 (Westlaw).

¹⁴¹ Compare § 423.508 (Westlaw), with 40/9 (Westlaw).

¹⁴² MICH. COMP. LAWS ANN. § 423.511 (West, Westlaw through P.A. 2011, No. 127, of the 2011 Regular Session, 96th Legislature); 820 ILL. COMP. STAT. 40/12 (West, Westlaw through P.A. 97-154, with the exception of P.A. 97-81 and P.A. 97-151, of the 2011 Reg. Sess.).

¹⁴³ 820 ILL. COMP. STAT. 40/5, 40/12(f) (West, Westlaw through P.A. 97-154, with the exception of P.A. 97-81 and P.A. 97-151, of the 2011 Reg. Sess.).

¹⁴⁴ See, e.g., Nicole B. Porter, *The Perfect Compromise: Bridging the Gap Between At-Will Employment and Just Cause*, 87 NEB. L. REV. 62 (2008); Stephen D. Sugarman, "Lifestyle" Discrimination in Employment, 24 BERKELEY J. EMP. & LAB. L. 377 (2003).

¹⁴⁵ N.D. CENT. CODE § 14-02.4-03 (2008); N.Y. LAB. LAW § 201-d (McKinney 1992).

¹⁴⁶ COLO. REV. STAT. § 24-34-402.5(1) (2007).

¹⁴⁷ N.D. CENT. CODE § 14-02.4-03 (2008).

That gives us the fact that we want to look at the ECPA, we want to look at the state statutes, and then of course we want to look at the invasion of privacy tort.

IV. TORT INVASION OF PRIVACY

In terms of invasion of privacy, we are all familiar with the tort of intrusion on seclusion. While it varies from state to state, the tort generally requires, first of all, that you have some reasonable expectation of privacy.¹⁴⁸ This needs to be subjectively, but more importantly, objectively reasonable.¹⁴⁹ There needs to be an intrusion on that expectation of privacy, and it should be highly offensive.¹⁵⁰ And that is objective. So the intrusion must be highly offensive in an objective way. This quotation is from *Smyth*, which is considered to be the seminal case in this area:

[W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of a urinalysis or personal property search to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.¹⁵¹

What happens here is that an employee uses profanity in communicating with his supervisor, and makes some really inappropriate remarks.¹⁵² But he has been told by management that none of the conversations and communications via the email system will be monitored.¹⁵³ Yet, lo and behold, there must have been reports of him making inappropriate comments because the managers decided to monitor, and they found these communications.¹⁵⁴ The court found that the employee had no reasonable expectation of privacy, despite the specific disclaimer that he would not be monitored.¹⁵⁵ As you see, significantly, this is not like a urinalysis or a search of personal property.¹⁵⁶ The court also went on to say that even if the employee had

¹⁴⁸ Corey A. Ciochetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 299 (2011).

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

¹⁵² *Id.* at 98-99.

¹⁵³ *Id.* at 98.

¹⁵⁴ *Id.* at 98-99.

¹⁵⁵ *Id.* at 101.

¹⁵⁶ *Id.*

some reasonable expectation of privacy, it is not highly offensive for an employer to investigate inappropriate comments in the workplace.¹⁵⁷

Nevertheless, at the same time, you will see the *Restuccia* case that came down around the same time.¹⁵⁸ This court said there could be a reasonable expectation of privacy.¹⁵⁹ There was an employer policy that said employees should not engage in excessive chat on the business email, but they could use it for personal communications.¹⁶⁰ The employee was accused of excessive quantity of email. The employee had been told that he could use the business email for personal communications; he had his own password, and he did not know supervisors could look at the emails.¹⁶¹ But it turned out that supervisors could take another password and go on and look at it, and look at everything that had been stored on the server.¹⁶² The court reasoned that there could be a reasonable expectation of privacy in those circumstances.¹⁶³ It was just denying summary judgment.¹⁶⁴ The court also said that the monitoring could be an “unreasonable, substantial or serious interference with plaintiffs’ privacy,”¹⁶⁵ a similar requirement to that of the highly offensive requirement in most jurisdictions.

Then we have *Fischer*, the case previously discussed about stored communications with the youth pastor, who also brought an invasion of privacy claim.¹⁶⁶ The court said, again on summary judgment, that “yes,” perhaps his Hotmail account was entitled to a reasonable expectation of privacy, and that it may have been highly offensive for his employer to go onto his personal account and read his emails.¹⁶⁷

Then there is the case *Thygeson*.¹⁶⁸ It comes to the opposite result of *Fischer*; it is consistent with *Smyth*. This is the case where an employee had nudity and sexually inappropriate jokes saved onto the computer.¹⁶⁹ He would go onto his personal email at work and download these things onto the computer and put them in

¹⁵⁷ *Id.*

¹⁵⁸ *Restuccia v. Burk Tech., Inc.*, No. CA 952125, 1996 WL 1329386 (Mass. Super. Ct. Aug. 13, 1996).

¹⁵⁹ *Id.* at *3.

¹⁶⁰ *Id.* at *1.

¹⁶¹ *Id.*

¹⁶² *Id.*

¹⁶³ *Id.* at *3.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ *Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 927-28 (W.D. Wis. 2002).

¹⁶⁷ *Id.*

¹⁶⁸ *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004).

¹⁶⁹ *Id.* at *3.

a file marked “personal.”¹⁷⁰ This court said that if you mark your file personal, but you do not restrict it with a password, you have no reasonable expectation of privacy in that file.¹⁷¹ The employer also investigated the Internet hits, not the content, just the pages the employee had hit, and the court again said there is no reasonable expectation of privacy in what Internet sites an employee hits.¹⁷² The court went on to find it would not be highly offensive.

I am still discussing the tort, and skipping to a different kind of observation. These cases come up all the time because of disability and workers’ compensation claims. What happens in this case, *I.C.U. Investigations, Inc.*,¹⁷³ is that you have an employee, and he obtained a \$100,000 judgment for invasion of his privacy because he had been injured.¹⁷⁴ The employer decided to investigate.¹⁷⁵ The employer hired I.C.U. to investigate the employee for 11 or 12 days.¹⁷⁶ The employee lived on a 41 acre yard,¹⁷⁷ but his yard was visible from a highway, and the I.C.U. investigators parked their car at the strip of the highway and videotaped what the employee was doing in the yard.¹⁷⁸ In particular, they videotaped him urinating four times in his yard.¹⁷⁹ So he obtained a \$100,000 judgment,¹⁸⁰ but, nevertheless, the Alabama Supreme Court was not impressed with the \$100,000 judgment. The court reasoned that he was out in his yard, and that was visible to the public, and so he had no reasonable expectation of privacy in his yard.¹⁸¹ There were dissents.¹⁸²

There are similar Ohio cases.¹⁸³ They are not as interesting in the facts, but the bottom line would be that employers do not observe people in their homes, but an employee has no reasonable expectation of privacy in what the employee is doing in the yard that is visible to an employer.¹⁸⁴

The Restatement of Employment is coming out.¹⁸⁵ It is a useful resource; it is going to have lots of areas and I suggest following its development. One of the areas

¹⁷⁰ *Id.* at *18.

¹⁷¹ *Id.* at *21.

¹⁷² *Id.* at *22.

¹⁷³ *I.C.U. Investigations, Inc. v. Jones*, 780 So. 2d 685 (Ala. 2000).

¹⁷⁴ *Id.* at 687.

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* at 690 (Cook, J., dissenting).

¹⁷⁸ *Id.* at 687.

¹⁷⁹ *Id.* at 688.

¹⁸⁰ *Id.* at 687.

¹⁸¹ *Id.* at 689-690.

¹⁸² *Id.* at 690-692.

¹⁸³ *York v. Gen. Elec. Co.*, 759 N.E.2d 865 (Ohio Ct. App. 2001); *Sowards v. Norbar, Inc.*, 605 N.E.2d 468 (Ohio Ct. App. 1992).

¹⁸⁴ *York*, 759 N.E.2d at 868; *Sowards*, 605 N.E.2d at 474.

¹⁸⁵ RESTATEMENT (THIRD) OF EMP’T LAW (Tentative Draft No. 3, 2011).

it is going to have is privacy. It is not out yet, but it is something that you want to look toward being aware of.

V. FOURTH AMENDMENT

Finally, we get to the Fourth Amendment—the moment we all have been waiting for, because the Fourth Amendment discussion involves *Quon*.¹⁸⁶ But it only applies in the public sector,¹⁸⁷ and that is why I save it for last. It is an additional thing that you need to be aware of if you are an employer or an employee in the public sector. We are probably all familiar with *O'Connor v. Ortega*¹⁸⁸ which is the backdrop to *Quon*. I'll just refresh your memory briefly on the case. Basically, you had a doctor, and he was placed on administrative leave.¹⁸⁹ The employer searched his office, his desk, and his file cabinets.¹⁹⁰ The Court could not reach a consensus, so it was a plurality opinion.¹⁹¹ Justice O'Connor wrote the decision,¹⁹² and the test that she adopted was a two-part test.¹⁹³ You look first at whether there was a reasonable expectation of privacy,¹⁹⁴ and second at whether the employer had violated it.¹⁹⁵ Scalia disagreed in his concurrence.¹⁹⁶ He does not like that test. He said there is always a reasonable expectation of privacy, just jump straight to the second part.¹⁹⁷

We hoped that in *Quon* we might get some clarification, but there is none. So the first thing you need to ask if you have one of these cases is what test and what result under either of these tests. As to whether you have a reasonable expectation of privacy, *Quon* was a situation where a SWAT Team officer was involved in some tryst, sending text messages of a sexual nature.¹⁹⁸ The employer decided to investigate because it thought that there was an overage every month, and there had been too much use of the equipment, and maybe it needed to raise the amount of messages that employees could send out.¹⁹⁹ The Court punted. The Court said it would not decide whether there was a reasonable expectation of privacy in those workplace electronic communications.²⁰⁰

¹⁸⁶ *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

¹⁸⁷ *Id.* at 2630.

¹⁸⁸ *O'Connor v. Ortega*, 480 U.S. 709 (1987).

¹⁸⁹ *Id.* at 712.

¹⁹⁰ *Id.* at 713-14.

¹⁹¹ *Id.* at 711.

¹⁹² *Id.*

¹⁹³ *Id.* at 715, 719.

¹⁹⁴ *Id.* at 715-19.

¹⁹⁵ *Id.* at 719-26.

¹⁹⁶ *Id.* at 729.

¹⁹⁷ *Id.* at 731-32.

¹⁹⁸ *City of Ontario v. Quon*, 130 S. Ct. 2619, 2625-26 (2010).

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 2630. There is a case that has since come down, *Warshak*, in the Sixth Circuit. The court found a reasonable expectation of privacy in electronic communications on an

What the Court did address was whether the intrusion was reasonable.²⁰¹ It said it was reasonable at the inception.²⁰² It is reasonable to look at text messages to determine how many text messages should be allotted to a person each month.²⁰³ It said that the scope of the investigation was also reasonable.²⁰⁴ The employees were on a SWAT Team; they should have known that their messages might be discoverable.²⁰⁵ That was one thing. The employer also took precautions. The managers looked at only two months' worth, not four or five months' worth, of messages.²⁰⁶ And when they got to the point of the internal investigation, they redacted all messages sent outside of work hours.²⁰⁷ You can think of slightly different facts that would change the outcome, so we don't know—there are a lot of open questions there.

VI. CONCLUSION

Finally, to wrap up, what might be done? There are a lot of laws here, but what might be done?

There is the possibility of federal legislation. There are a lot of people pushing for a federal privacy law. A broad coalition of groups, including Microsoft and the Center for Democracy and Technology, are pushing for a European style data-protection law.²⁰⁸ The proposed Boucher Bill is such legislation,²⁰⁹ although it does not focus on employment.²¹⁰ Some have called for a sectoral approach,²¹¹ which could include a federal law aimed at privacy issues raised in the employment sector. If you predominately represent employers, and are concerned about differing rules from jurisdiction to jurisdiction, you can get involved with promoting preemptive federal legislation. And, if you predominately represent employees and desire European-style minimum rights, then you can get involved with promoting a federal data-protection law. Whomever you represent, you can figure out whether you prefer an omnibus or sectoral approach to federal legislation.

internet service provider (ISP). It is not a workplace case, but you might want to be aware of it. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

²⁰¹ *Quon*, 130 S. Ct. at 2630.

²⁰² *Id.* at 2631.

²⁰³ *Id.*

²⁰⁴ *Id.*

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904 (2009).

²⁰⁹ Staff Discussion Draft (2010), available at http://www.infolawgroup.com/uploads/file/Boucher%20Privacy_Draft_5-10.pdf.

²¹⁰ Since the lecture, Senator Leahy has introduced proposed amendments to the ECPA. Elec. Commc'ns Privacy Act, S. 1011, 112th Cong. (2011), available at <http://leahy.senate.gov/imo/media/doc/BillText-ElectronicCommunicationsPrivacyActAmendmentsAct.pdf>.

²¹¹ Schwartz, *supra* note 208.

There is also the possibility of state legislation. Much like there was tort reform with workers' compensation, the possibility exists that there could be some consensus among the constituencies in a particular state. The states with notice laws, off-duty activity laws, and laws governing the integrity of personnel records might be models to consider for those in other states.

As to what might be done on a more case-by-case basis, there is a lot of activity in terms of the union setting with collective-bargaining agreements. I actually spend a lot of time studying arbitration and reading labor arbitration opinions and awards. Interestingly, the labor arbitrators are grappling with a lot of these privacy issues.²¹² These issues come up when an employee is terminated, arguably in violation of a just cause provision or when a union bargains over a policy that impacts employer electronic monitoring. So, one idea, if you represent unions or employers in the unionized sector, is that they can bargain for certain policies or use arbitration as a way to develop a coherent agreement about these monitoring and privacy issues.

Even in the non-union sector, there are employer-promulgated policies, which are important. We have seen that these policies are encouraged by the ECPA because of the consent and user authorization exceptions. And these policies can impact whether an employee has a reasonable expectation of privacy in electronic communications sent while at work or using an employer's equipment. It is a good idea for those who predominately represent employers to encourage review of these policies. They should be reviewed not only in light of these laws, but also in light of the psychological literature about whether monitoring is appropriate for a particular workforce, and, if so, how it should be carried out.²¹³

Finally, in terms of education, I encourage you to join the ABA Labor and Employment Law Section that has a committee on technology in the workplace. They do great work around these issues.²¹⁴ And, of course, there are many other organizations in which you can become involved. The American Civil Liberties Union has been active in privacy for employees for a long time.²¹⁵ The Future of Privacy Forum,²¹⁶ which is a think tank in D.C., is involved in the Boucher legislation. I encourage you to talk to your friends and colleagues. People do not realize that they are susceptible to monitoring or that information is not private. Employers do not realize there are all these laws they could run afoul of.

So consider a glass, and the question is: is it half empty or half full? If you have been thinking through the questions that were posed, you might say it is half empty.

²¹² See Levinson, *supra* note 2. See also Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609 (2009).

²¹³ See, e.g., John R. Aillo & Kathryn J. Kolb, *Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress*, 80 J. APPLIED PSYCHOL. 339, 349 (1995); Pascale Carayon, *Effects of Electronic Performance Monitoring on Job Design and Worker Stress: Results of Two Studies*, 6 INT'L J. HUM. COMPUTER INTERACTION 177, 185, 186 (1994).

²¹⁴ *Section of Labor and Emp't Law*, AMERICAN BAR ASSOCIATION, <http://apps.americanbar.org/dch/committee.cfm?com=LL100950> (last visited Sept. 15, 2011).

²¹⁵ *Workplace Privacy*, AMERICAN CIVIL LIBERTIES UNION, <http://www.aclu.org/technology-and-liberty/workplace-privacy> (last visited Sept. 15, 2011).

²¹⁶ FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/?gclid=CNLp6_7IvakCFUnr7QodLS32gw (last visited Sept. 15, 2011).

There are all these different protections; employers don't know what to apply; they don't know what safe harbor is. Employees cannot tell if there is some type of minimal right. Or you might say it is half full. You might think "there is a lot more here than I thought before I stepped in the room today that is applicable in this setting." And perhaps both are true. Thank you for your time.