WORKPLACE PRIVACY AND MONITORING: THE QUEST FOR BALANCED INTERESTS

Ariana R. Levinson*

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—they can easily take their office home with them. And 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.

And so for employers this raises a number of concerns.[2] First of all, employee could be spending an inordinate amount of time doing personal tasks in the workplace.[3] Second, some of the tasks they may be doing may be inappropriate for the workplace. They may be looking at child pornography,[4] or they may be engaging in messaging that may be considered sexual harassment.[5] Finally, it is very easy, at the push of the button, to put information out to the public at this point. This might happen inadvertently or it might happen purposely. Those of you who predominantly represent employers can probably think of some other difficulties that the 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 because of the advancing technology[6]—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 that when monitoring is engaged in certain ways it

---

*Assistant Professor, University of Louisville, Louis D. Brandeis School of Law; J.D., University of Michigan Law School. This article is a transcript, with several asides deleted and with 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 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 & Private Lives*, 66 LA. L. REV. 1035, 1037 n.8 (2006).

[2] *See* Ariana R. Levinson, *What Hath the Twenty First Century Wrought? Issues in the Workplace Arising from New Technologies & 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] Levinson, *supra* note 2, at 7

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 this one from the AMA, the American Management Association, because they have done this three times.[8] They have collected data—it 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% 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 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, 12% of the reporting employers were monitoring the blogosphere, 8% were monitoring GPS vehicle tracking, and 10% were monitoring social networking sites[12]. Probably, some of you are working with social networking policies with the companies that you are involved with. That is a hot topic right now. And so 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 computer.[14] Or, it can be software. If it is software, it creates a printout. It logs every keystroke that the employee is making, so the

---

[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] AMA/EPOLICY INST. RESEARCH, AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY (2008) , *available at* http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.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] Finkin, *supra* note 8, at 474.

[11] *Compare* AMA/EPOLICY INST. RESEARCH, AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY (2008) , *available at* http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf, *and* Finkin, *supra* note 8, at 474.

[12] AMA/EPOLICY INST. RESEARCH, AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY (2008) , *available at* http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf

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

[14] *Id.*

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 they have 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 does capture this information contemporaneously.

So that just 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 are also some state statutes that are going to be relevant in various different states. There is the tort that we are all very familiar with, dating back to Brandeis's days, of the invasion of privacy, invasion of seclusion.[20] And then finally we know 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, though, 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: is there some sort of safe harbor here? If the employer is trying to protect employees' privacy and also meet the needs that it needs to meet, 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

---

[15] *Id.*
[16] Hayes v. Spectorsoft 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] 18 U.S.C. §§ 2510–22 (2008).
[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 Baltimore, 118 A. 77 (Md. 1922); Judevine v. Benzies-Montanye Fuel & Warehouse Co., 269 N.W. 295 (Wis. 1936).
[21] 130 S. Ct. 2619 (2010).

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 us—legal advice—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 does feel that privacy has been invaded? So we can think of all these questions as we are looking at these laws.

II. ECPA

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 that is out there.[23] And having spent the last year and a half looking at it, I throw my weight in 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 nut shell view so you can have some base-line understanding of what's involved with the ECPA.

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 in here 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. It is the interception of electronic

---

[22] 18 U.S.C. §§ 2510–22.

[23] Steve Jackson Games, Inc. v. U. S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) ; 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); Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 866 (2002 ; Jeremy E. Gruber & Lewis Maltby, *The Need for Reasonable Policies*, 213 FEB. N.J. LAW. 41, 43 (2002); Connie Barba, *"That's No 'Beep', That's My Boss": Congress Seeks to Disconnect the Secrecy of Telephone Monitoring in the Workplace*, 21 JOHN MARSHALL L. REV. 881, 883 n.17 (1988); 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).

[24] 18 U.S.C. §§ 2510–22, 2701–12, 3121–27.

[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).

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 that 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 Act[30] that we are 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. We will not go into all of them, but we will take 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 1980's 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 and 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. And at most of the time they are passing from sender and 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

---

[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).
[31] The issues are 1) interception; 2) consent; 3) provider; 4) ordinary course of business; and, 5) interstate commerce.
[32] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 886–87 (9th Cir. 2002) (J. Reinhardt, dissenting).

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 you could send text messages through the paging system.[35] You could do this in one of three ways if you were an employee.[36] You could do it through your 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] You would type the message on to the employer's computer. It would go off then 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: were these messages "intercepted" when the computer acquired them 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 communications. That was the traditional view.

More recently you have *Global Policy Partners*, a 2009 case.[45] 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 it can be stored and still intercepted. They still, however, want it to be during transmission to constitute an interception. So in *Global Policy* you had a husband and wife team—these cases all make for interesting facts—and they were working in a company, and then they decided to separate and divorce.[46] And so 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,

---

[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 v. City of Reno, 932 F. Supp.1232 (D. Nev. 1996).
[35] *Id.* at 1233–34.
[36] *Id.* at 1234.
[37] *Id.*
[38] *Id.* at 1233.
[39] *Id.* at 1234.
[40] *Id.*
[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).
[46] *Id.* at 633.
[47] *Id.* at 634.

which she does, is: is this 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]

So 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 does this 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."

---

[48] *Id.* at 637.
[49] *Id.* at 638.
[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

So once you have an interception—you have determined an employer has intercepted somebody's electronic communications – next you check whether the employer fits into any of the exceptions—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, pre-electronic communication—a long history of what consent means.[58] It is very explicit in the legislative history: this is implied consent, implied-in-fact consent. You have to look at the actual facts,[59] consider the totality of the circumstance, and determine: did the person know he or she was being monitored and did the person assent. 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 more tricky. It only applies when you are using telephone and telegraph equipment generally.[62] The Second Circuit has ruled otherwise, though.[63] They apply 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 is containing 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] In the Sixth Circuit, which we

---

[57] Ariana 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* United States v. Townsend, 987 F.2d 927 (2nd 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 (3rd 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, 2007 WL 539534, *8 (S.D. Ohio 2007).
[61] Levinson, *supra* note 57 at 34.
[62] Levinson, *supra* note 57 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., Inc., 630 F.2d 414, 420 (5th Cir. 1980).

are interested in here,[67] they require a legitimate business reason., they require that it be in the ordinary course of things, a routine practice, and they require notice.[68] So they are the most stringently restrictive in terms of the ordinary course of business exception.

The courts are also all over the map on whether 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.[69] Others say you should stop: when you hear "hi, honey" on the telephone, stop monitoring.[70] These cases are all over the map.

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 . . . ."[71]

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.[72] So we have courts that have interpreted this more or less broadly. In specific, this language "rights or property" of the employer has been interpreted more or less broadly. So you have the *Kinesis* case.[73] This comes from North Carolina.[74] In this case, there was an employee who left and had breached, or allegedly breached, a covenant not to compete.[75] 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

---

[67] Just like in Kentucky and in Michigan, even if we don't like Michigan, we want to know what the Sixth Circuit thinks.
[68] *Adams*, 250 F.3d at 984.
[69] Amati v. City of Woodstock, 176 F.3d 952, 956 (7th Cir. 1999).
[70] *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983).
[71] 18 U.S.C. 2511(2)(a)(i) (2008).
[72] *Id.*
[73] Kinesis Adver., Inc. v. Hill, 652 S.E.2d 284 (N.C. Ct. App. 2007).
[74] *Id.*
[75] *Id.* at 289.

compete.[76] The court said "yes," that is protection of the employer's rights and property.[77] So, that employer acted lawfully and did not violate the Wiretap Act.[78]

And then with an even broader interpretation of this language, we have *Freedom Calls*.[79] Here, the employee was terminated, and the employer went back again into the business email and responded to the messages that were coming in, using the employee's email account on the employer's business email.[80] The court here took an even broader approach. The court said "yes," the employer was the provider.[81] The court reasoned that the employer needed to timely respond to messages and needed to make sure that the business acted efficiently, and so this falls in the protection of the rights or property of the employer.[82]

But there is an interesting case, *O'Grady*, a California case,[83] 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.[84] But what it is interesting is that that court drew a very firm line saying that "rights or property" does not mean any cost to the employer.[85] 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. [86] 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,

So that is the Wiretap Act. You want to ask yourself is it an interception, and if so, does the employer fall within one of the exceptions.

B. Stored Communications Act

Then we get to the Stored Communications Act.[87] It is exactly the same—it is really complicated; it has all these issues (you can see them listed out)[88]; and the courts have gone every which way again on all of them.

---

[76] *Id.* at 296.
[77] *Id.*
[78] *Id.*
[79] Freedom Calls Found. v. Bukstel, 2006 WL 845509 at *27 (E.D.N.Y. March 3, 2006).
[80] *Id.* at *3.
[81] *Id.* at *27
[82] *Id.*
[83] O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72 (2006).
[84] *Id.* at 1440–1451.
[85] *Id.* at 1441–42.
[86] Levinson, *supra* note 57, at 37.
[87] 18 U.S.C. §§ 2701–2712 (2008).
[88] The issues are: 1) electronic storage; 2) without authorization; 3) obtains, alters, prevents authorized access; 4) provider exemption, and; 5) user authorization.

1. Electronic Storage

The first question we encounter here is: what is a stored communication? The Act prohibits unauthorized access to stored communications.[89] 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) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[90]

Most courts have said this is very broad.[91] If an ISP provider has the electronic communication, that is a stored communication. But, not all of them.

One good example of a court interpreting the language broadly is the *Fischer* case.[92] In this case, a church that was the employer of a youth pastor.[93] The youth pastor's obligations were to counsel youth but also periodically adults.[94] Somebody thought that they overheard a sexual conversation between the youth pastor and another male adult.[95] The employer was concerned about this, and decided to investigate. The employer hired an expert.[96] The expert went on to the work computer and guessed at what the hotmail account password of the employee was.[97] 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.[98] The employer went into the account, read the messages, and printed some of them out.[99] The first question is: were those stored communications? The court said "yes."[100] The court reasoned the messages were there on the hotmail server, they were stored there, and that was a stored communication.[101]

But there are other courts, and these are a minority, that have said "no," the term "electronic storage" is not that broad. In particular, there is an interesting

---

[89] 18 U.S.C. § 2701.
[90] 18 U.S.C. §2510(17) (2008).
[91] Levinson, *supra* note 57, at 51.
[92] Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wis. 2002).
[93] *Id.* at 917.
[94] *Id.*
[95] *Id.* at 918.
[96] *Id.* at 920.
[97] *Id.*
[98] *Id.* at 917.
[99] *Id.* at 920.
[100] *Id.* at 925–26.
[101] *Id.* at 925.

case, the *Flagg* decision.[102] The *Flagg* decision is out of the Eastern District of Michigan, and it has complicated facts. What it boils down to is the whether messages created by employees of a city were in electronic storage.[103] The city had a text messaging service, and it stopped using it.[104] But the service continued to retain copies of those messages.[105] The question was: were those stored? The court said "no."[106] The court reasoned that the copy retained by the service was the only copy, and the only copy cannot be a backup copy.[107] So the court held the messages weren't stored. And you will see other cases going both ways.[108]

2. Exceptions

There are two exceptions. We are not going to go into "Without Authorization." It has a lot of case law.[109] 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."[110] Notice how much more broad it is in the language than the provider exception we saw 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.[111] Now, if it is a third party provider, then that is different, like with the text messaging companies.[112] That gets into the distinction between

---

[102] Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).
[103] *Id.*at 361.
[104] *Id.* at 347–48.
[105] *Id.* at 348.
[106] *Id.* at 362.
[107] *Id.* at 362–63.
[108] Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (stored); KLA-Tencor Corp. v. Murphy, 2010 WL 1912029, at *8 (N.D. Cal. May 11, 2010) (assuming without deciding that not stored); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (stored); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (stored).
[109] See e.g. the following cases discussing authorization, Monson v. Whitby School, Inc. 2010 WL 3023873, at *5 (D. Conn. Aug. 2, 2010); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (S.D.N.Y. 2008); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008); Wyatt Technology Corp. v. Smithson, 2006 WL 5668246, at *9 (C.D. Cal. Aug. 14, 2006) *aff'd in relevant part*, 345 Fed. Appx. 236 (9th Cir. Aug. 27, 2009); Global Policy Partners v. Yessin, 686 F. Supp. 2d 631, 636 (E.D. Va. Nov. 24, 2009); Borninski v. Williamson, 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).
[110] 18 U.S.C. § 2701(c)(1)
[111] See Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 115 (3d Cir. 2004); Freedom Calls Found. v. Bukstel, 2006 WL 845509, at *27 (E.D.N.Y. March 3, 2006).
[112] Levinson, *supra* note 57 at 52, 56.

electronic communications services and remote computing services. We won't talk about those today, but that distinction determines when dealing with third party provider, whether the third party provider can release the electronic communication to the employer or not.[113]

The exception that has some interesting cases is the "user authorization" exception. And it is interesting because you have here 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 get user authorization. One interesting case is *Pure Power Boot Camp*.[114] This employee did something we should all 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.[115] When he accessed his Hotmail account, he used that function to "remember my password."[116] Don't use that function. So he left it 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.[117] So the employer had a policy; 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."[118] 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.[119] 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?[120] The court reasoned that even in the face of this policy, that is not user authorization.[121]

The other issue that comes up in these user authorization cases is illustrated by *Pietrylo*.[122] What happened here is that employees were using a chat group.[123] The case does not reflect what was on there, but I imagine it was disparaging of the

---

[113] *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) *cert. denied* 130 S. Ct. 1011 (Dec. 4, 2009).
[114] Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).
[115] *Id.*at 552.
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.* at 561–62.
[120] *Id.* at 561.
[121] *Id.* at 562.
[122] Pietrylo v. Hillstone Rest. Group, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).
[123] *Id.* at *1.

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.[124] But the court found that was not user authorization because the employee felt pressured to give the manager the password.[125] The employee felt that if she hadn't given it to the manager, there would have been negative consequences.[126] So again, that was not found to be user authorization.

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

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 you don't seem to have two-party consent, so yours is like the one we just discussed.[127] 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,[128] whereas Rhode Island just prohibits video or audio in the restroom.[129]

There are also a couple states, Connecticut[130] and Delaware,[131] that have notice laws. These are modeled on the NEMA – Notice of Electronic Monitoring Act – that failed to pass around 2000.[132] It was a proposed federal statute. So these again are based on that same concept, most likely,[133] that employers are more reflective when they need to provide notice. They think more about how to monitor. And employees have that opportunity to change their behavior. There are differences again in between the two states. The Connecticut statute is really

---

[124] *Id.* at *1, *3.
[125] *Id.*
[126] *Id.*
[127] Ohio Rev. Code Ann. § 2933.52 (West, Westlaw through 2011 Files 1 - 19, of the 129th GA (2011-2012)).
[128] N.Y. LABOR LAW § 203-c (West, Westlaw through L.2011, chapters 1 to 18 and 50 to 54).
[129] R.I. GEN LAWS § 28-6.12-1 (West, Westlaw through chapter 321 of the January 2010 session).
[130] CONN. GEN. STAT. § 31-48d (2008).
[131] DEL. CODE ANN. tit. 19, § 705 (2008).
[132] Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000).
[133] The Acts do not explicitly state the concept on which they are based.

broad. You need to give notice of any kind of monitoring that is not direct observation.[134] The Delaware statute is more limited: it covers monitoring of telephone, internet, and email.[135] Connecticut requires written notice.[136] In Delaware, it is okay to have something that pops up on the screen when the employee logs in and that could be the form of notice that is provided.[137] Connecticut has a labor commissioner proceeding.[138] In Delaware, you file individual suit.[139] So as you are thinking about ideally what would work here, 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, some of these neighboring states, there are acts that govern the integrity of personnel records.[140] So again these are not specifically geared towards electronically monitoring and monitoring, but what they prohibit is gathering information about people's non-employment related communication.[141] And of course if the employee authorizes this, it is alright in both of these states, but, in that instance, you would need to have a record of what you gathered as an employer, and a right for the employee to review the information.[142] 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.[143] Michigan has a lawsuit; Illinois has the Department of Labor.[144] Illinois includes anti-retaliation provisions and provisions that give union representatives the right to review information.[145]

These are interesting statutes: lawful off-duty activity statutes. Several scholars have written about them.[146] You may have heard them referred to as life-style discrimination statutes. What the goal of these statutes is, 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

---

[134] CONN. GEN. STAT. § 31-48d.
[135] DEL. CODE ANN. tit. 19, § 705.
[136] CONN. GEN. STAT. § 31-48d.
[137] DEL. CODE ANN. tit. 19, § 705.
[138] CONN. GEN. STAT. § 31-48d..
[139] DEL. CODE ANN. tit. 19, § 705.
[140] MICH. COMP. LAWS § 423.508 (West, Westlaw through P.A. 2011, No.64 (except 62), of the 2011 Regular Session, 96th Legislature); 820 ILL. COMP. STAT. 40/9 (West, Westlaw through P.A. 97-13, with the exception of P.A. 97-6, of the 2011 Reg. Sess).
[141] MICH. COMP. LAWS § 423.508; 820 ILL. COMP. STAT. 40/9.
[142] MICH. COMP. LAWS § 423.508; 820 ILL. COMP. STAT. 40/9.
[143] *Compare* MICH. COMP. LAWS § 423.508 *with* 820 ILL. COMP. STAT. 40/9.
[144] MICH. COMP. LAWS § 423.511; 820 ILL. COMP. STAT. 40/12.
[145] 820 ILL. COMP. STAT. 40/5, 40/12(f).
[146] 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).

coverage of them. In North Dakota and New York the prohibition is pretty broad—any type of adverse action.[147] In Colorado, it is just prohibiting termination because of lawful off-duty conduct.[148] In North Dakota the coverage is broad, it is any type of lawful off-duty conduct.[149] 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, that might fall within the protections of the New York statute. The exceptions in the enforcement provisions vary.

So 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 tort, 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.[150] This needs to be subjectively but, more importantly, objectively reasonable.[151] There needs to be an intrusion on that expectation of privacy, and it should be highly offensive.[152] And that is objective again. So highly offensive in an objective way. This quote is a quote 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 an urinalysis or personal property search to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over

---

[147] N.D. CENT. CODE § 14-02.4-03 (2008).; N.Y. LAB. LAW § 201-d (McKinney 1992).
[148] COLO. REV. STAT. § 24-34-402.5(1) (2007).
[149] N.D. CENT. CODE § 14-02.4-03 (2008).
[150] Corey A Ciochetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 299 (2011).
[151] *Id.*
[152] *Id.*

> the company e-mail system. We find no privacy interests in such communications.[153]

So what happens here is an employee uses profanity in communicating with his supervisor, and makes some really inappropriate remarks.[154] But he has been told by management that none of the conversations and communications via the email system will be monitored.[155] Yet, low and behold, there must have been reports of him making inappropriate comments because the managers decide to monitor, and they find these communications.[156] And the court finds that the employee had no reasonable expectation of privacy despite the specific disclaimer that he would not be monitored.[157] As you see, significantly, this is not like a urinalysis or a search of personal property.[158] The court also went on to say that even if the employee had some reasonable expectation of privacy, it is not highly offensive for an employer to investigate inappropriate comments in the workplace.[159]

Nevertheless, at the same time, you will see the ***Restuccia*** case, that came down around the same time.[160] This court said there could be a reasonable expectation of privacy.[161] Here the court said 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.[162] 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 own password; and he did not know supervisors could look at the emails.[163] But it turned out supervisors could take another password and go on and look at it, and look at everything that had been stored on the server.[164] And the court reasoned that there could be a reasonable expectation of privacy in those circumstances.[165] It was just denying summary judgment.[166] And the court also said that the monitoring could be "unreasonable, substantial or serious interference with plaintiffs' privacy," a similar requirement to that of the highly offensive requirement in most jurisdictions.

---

[153] Smyth v. Pilsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).
[154] *Id.* at 98–99.
[155] *Id.* at 98.
[156] *Id.* at 98–99,
[157] *Id.* at 101.
[158] *Id.*
[159] *Id.*
[160] Restuccia v. Burk Tech., 1996 WL 1329386 (Mass. Super. Ct. Aug. 13, 1996).
[161] *Id.* at *3.
[162] *Id.* at *1.
[163] *Id.*
[164] *Id.*
[165] *Id.* at *3.
[166] *Id.*

Then we have *Fischer*, the case that we just talked about with stored communications with the youth pastor, who also brought in an invasion of privacy claim.[167] 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.[168]

Then we have the case *Thygeson*.[169] 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.[170] He would go onto his personal email at work and download these things onto the computer and put them in a file marked "personal."[171] So 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.[172] And 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 you hit.[173] They went on to find it would not be highly offensive.

We're still in the tort, and we are skipping to a different kind of observation. These cases come up all the time because of disability and worker's compensation claims. So what happens in this case, *I.C.U. Investigations, Inc.*,[174] you have an employee, and he obtains a $100,000 judgment for invasion of his privacy because he has been injured.[175] The employer decides to investigate.[176] The employer hires I.C.U. to investigate him for eleven or twelve days.[177] He lives on a forty-one acre yard,[178] but his yard is visible from a highway, and the I.C.U. investigators park their car at the strip of the highway and videotape what the employee is doing in the yard.[179] In particular, they videotape him urinating four times in his yard,[180] so he obtains a $100,000 judgment,[181] but, nevertheless, the Alabama Supreme Court is not impressed with the $100,000 judgment. The court reasons that he was out in

---

[167] *Fischer*, 207 F. Supp. 2d at 927–28.
[168] *Id.*
[169] Thygeson v. U.S. Bancorp, 2004 WL 2066746 (D. Or. Sept. 15, 2004).
[170] *Id.* at *3.
[171] *Id.* at *18.
[172] *Id.* at 21.
[173] *Id.* at 22.
[174] I.C.U. Investigations, Inc. v. Jones, 780 So.2d 685 (Ala. 2000).
[175] *Id.* at 687.
[176] *Id.*
[177] *Id.*
[178] *Id.* at 690 (Cook, J., dissenting).
[179] *Id.* at 687.
[180] *Id.* at 688.
[181] *Id.* at 687.

his yard, and that was visible to the public, and so he had no reasonable expectation of privacy in his yard.[182] There were dissents.[183]

There are similar Ohio cases.[184] They are not as interesting in the facts, but the line would be you do not observe people in their home, but you have no reasonable expectation of privacy in what you are doing in your yard that is visible to your employer.[185]

The Restatement of Employment is coming out.[186] It is a useful resource; it is going to have lots of areas; and I suggest following its development. One of the areas it is going to have is privacy. It is not out yet, but it is something that you want to look towards 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 has *Quon*.[187] But it only applies in the public sector,[188] and that is why I save it for last. It is an additional thing that if you are an employer or an employee in the public sector, you need to be aware of. We are probably all familiar with *O'Connor v. Ortega*[189] 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.[190] The employer searched his office, his desk, and his file cabinets.[191] The court could not reach consensus, so it was a plurality opinion.[192] Justice O'Connor wrote the decision,[193] and the test that she adopted was a two part test.[194] You would look first at whether there was a reasonable expectation of privacy,[195] and second whether the employer had violated it.[196] Scalia disagreed in his concurrence.[197] He does not like that test. He

---

[182] *Id.* at 689–690.
[183] *Id.* at 690–692.
[184] 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).
[185] *York*, 759 N.E.2d at 868; *Sowards*, 605 N.E.2d at 474.
[186] Information is available at http://www.ali.org/index.cfm?fuseaction=projects.proj_ip&projectid=11.
[187] City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
[188] *Id.* at 2630.
[189] 480 U.S. 709 (1987).
[190] *Id.* at 712.
[191] *Id.* at 713–14.
[192] *Id.* at 711.
[193] *Id.*
[194] *Id.* at 715, 719.
[195] *Id.* at 715–19.
[196] *Id.* at 719–26.
[197] *Id.* at 729.

said there is always a reasonable expectation of privacy, just jump straight to the second part.[198]

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 you had a SWAT Team officer involved in some tryst, sending text messages of a sexual nature.[199] The employer decides to investigate because it thinks that there is an overage every month, and there has been too much use of the equipment, and maybe it needs to raise the amount of messages that employees can send out.[200] The court punts. The court says we will not decide whether there is a reasonable expectation of privacy in those workplace electronic communications.[201]

So what the court did address was whether the intrusion was reasonable.[202] They said it was reasonable at the inception.[203] It is reasonable to look at text messages to determine how many text messages should be allotted to a person each month.[204] They said that the scope of the investigation was also reasonable.[205] The employees were on a SWAT Team; they should have known that their messages might be discoverable.[206] 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.[207] And when they got to the point of the internal investigation, they redacted all messages sent outside of work hours.[208] 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

So finally, to wrap up, what might be done? We have 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 the

---

[198] *Id.* at 731–32.
[199] *Quon*, 130 S. Ct. at 2625–26.
[200] *Id.*
[201] *Id.* at 2630. There is a case that came down since, *Warshak*, in the Sixth Circuit. They found a reasonable expectation of privacy in electronic communications on an ISP provider. It is not a workplace case, but you might want to be aware of it. United States v. Warshak, 2010 WL 5071766, at *14 (6th Cir. Dec. 14, 2010).
[202] *Quon*, 130 S. Ct. at 2630.
[203] *Id.* at 2631.
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*

Microsoft and the Center for Democracy and Technology, are pushing for a European style data-protection law.[209] And the proposed Boucher Bill is such legislation,[210] although it does not focus on employment.[211] Some have called for a sectoral approach,[212] which could include a federal law aimed at privacy issues raised in the employment sector. So, 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.

There is also the possibility of state legislation. So much like there was tort reform with workers compensation, the possibility exists here, 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 for those in other states to consider.

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.[213] 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 between themselves 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

---

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

[210] Staff discussion draft available at http://www.infolawgroup.com/uploads/file/Boucher%20Privacy_Draft_5-10.pdf.

[211] Since the lecture, Senator Leahy has introduced proposed amendments to the ECPA. The proposal focuses on government monitoring and is available at http://leahy.senate.gov/imo/media/doc/BillText-ElectronicCommunicationsPrivacyActAmendmentsAct.pdf.

[212] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009)

[213] *See* Ariana R. Levinson, *What Hath the Twenty First Century Wrought? Issues in the Workplace Arising from New Technologies & How Arbitrators Are Dealing with Them*, 11 TRANSACTIONS: TENN J. OF BUS. L. 9 (2010); Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & P. POL'Y 609 (2009).

equipment. It is a good idea for those who are or 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.[214]

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.[215] And, of course, there are many other organizations in which you can become involved. The ACLU has been active in privacy for employees for a long time.[216] The Future of Privacy Forum,[217] which is a think-tank in D.C., is involved in the Boucher legislation. I encourage you just to talk to you 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 we posed, you might say it is half empty. 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.

---

[214] *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).

[215] Information is available at http://apps.americanbar.org/dch/committee.cfm?com=LL100950.

[216] Information is available at http://www.aclu.org/technology-and-liberty/workplace-privacy.

[217] Information is available at http://www.futureofprivacy.org/?gclid=CNLp6_7IvakCFUnr7QodLS32gw.