Minnesota Journal of Law, Science & Technology

Volume 15 | Issue 2 Article 6

2014

The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era

Lisa M. Durham Taylor

The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era

Lisa M. Durham Taylor*

ABSTRACT

When it comes to employee privacy rights in emerging technologies, the times they are a-changin'. In the dawn of the modern technological era, when electronic mail and the Internet were in their relative infancy, the right to privacy meant almost nothing in the workplace. Employers could promise that e-mail would not be monitored, but then proceed to do so anyway. When employees sued, seeking vindication of their perceived privacy rights, courts cast aside any notion that an employee could expect privacy in the workplace, and they did so almost uniformly. The tide, however, appears to be turning. Judicial decisions rendered in more recent years, coupled with comparable statutory reform initiatives, suggest that as social norms shift in light of the rapid development and mainstreaming of modern technologies, the law is affording protection to employees that previously did not exist. This Article takes a retrospective-comparative approach to this turning tide, delving deeply into the law of the early era of modern technology and juxtaposing it against more recent developments. The result is exposition of an unmistakable trend favoring employee rights. This Article therefore tackles head-on the ultra-modern legal problem of workplace privacy rights in emerging technologies, but it does so in novel ways, as the first to suggest that the trend is shifting toward greater recognition of employee rights at the expense of employer prerogative.

---

* Associate Professor, Atlanta's John Marshall Law School, Atlanta, Georgia.

Come senators, congressmen
Please heed the call
Don't stand in the doorway
Don't block up the hall
For he that gets hurt
Will be he who has stalled
There's a battle outside
And it is ragin'
It'll soon shake your windows
And rattle your walls
For the times they are a-changin'.[1]

INTRODUCTION

The "ragin' battle" in this case is not one that Bob Dylan contemplated. Indeed, no one alive at the time he first swooned those lyrics could have predicted the future that is now. The "battle" involves the likes of iPhones and iPads, Blackberries and laptops, Hotmail and Gmail, Facebook and Twitter—technologies that could not even be fathomed fifty years ago, but which are pervasive parts of the American economy today.[2] Given their pervasiveness, it comes as no surprise that these technologies permeate the workplace.[3] This is both a blessing

---

1. BOB DYLAN, *The Times They Are a-Changin'*, *on* THE TIMES THEY ARE A-CHANGIN' (Columbia Records 1963), *quoted in* City of Ontario v. Quon, 560 U.S. 746, 768 (2010) (Scalia, J., concurring) (criticizing the majority opinion for avoiding direct confrontation of the question of the Fourth Amendment's application to new workplace technologies, chastising, "[t]he-times-they-are-a-changin' is a feeble excuse for disregard of duty").

2. That such technologies are pervasive is indubitable. Nevertheless, a multitude of statistics are available to support this assertion. For example, a leading consumer research firm, The Nielsen Company, recently reported that thirty-seven percent of all mobile customers in the United States have smartphones (Blackberry, iPhone, etc.). *Android Leads in U.S. Smartphone Market Share and Data Usage*, NIELSEN (May 31, 2011), http://blog.nielsen.com/nielsenwire/consumer/android-leads-u-s-in-smartphone-market-share-and-data-usage.html. Facebook reports that it has over 900 million users, over 700 million of whom are daily active users. *See* FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Mar. 1, 2014); *cf.* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 654 (N.J. 2010) ("In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail.").

3. *See* Alison Diana, *Workplace Social Network, Personal Device Use Gaining*, INFORMATIONWEEK (June 24, 2010, 11:54 AM), www.informationweek.com/news/windows/microsoft_news/225701319 (discussing pervasive, and growing, use of social networking sites and

and a curse. On one hand, employers reap a multitude of benefits from employee use of technologies, including increased productivity, efficiency, connectivity, and even morale, among others.[4] On the other hand, with workers instantly connected to the outside world, employers risk disclosure of trade secrets and confidential information.[5] Employee online activities offer a new frontier for workplace harassment, exposing employers to liability in ways that are difficult to monitor and control.[6] The lines separating an employee's work from her life outside the office are becoming ever more blurry, as she forges virtual

---

personal devices at work, and hypothesizing eventual demise of workplace bans on such activity); *Yammering Away at the Office: A Distraction or a Bonus?*, THE ECONOMIST (Jan. 28, 2010), www.economist.com/node/15350928 (stating that with the advent of cloud computing and offerings from firms like Apple, Facebook, and Google, consumers now have widespread access to communications devices and web applications that they can use from the workplace); *see also Stengart*, 990 A.2d at 655 ("In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.").

4. *Cf.* IAN C. BALLON, E-COMMERCE & INTERNET LAW § 58.09[2] (Supp. 2013–14) ("Any policy should be drafted to be consistent with a company's corporate culture. Policies also should be written with an eye towards their intended effect on employee morale."); Ariel D. Cudkowicz et. al., *Technology and Privacy in the Workplace: Monitoring Employee Communications After the Supreme Court's* Quon *Decision*, BOS. B.J., Fall 2010, at 29, 29 ("[E]mployees are regularly encouraged or required to perform their job duties using employer-provided technologies, such as computers, PDAs, and e-mail, and employers often explicitly permit or tolerate limited use of workplace resources to access personal e-mail accounts, commercial websites, and social networking sites.").

5. *See, e.g.*, Sasqua Grp., Inc. v. Courtney, No. CV 10-528(ADS)(AKT), 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010) (discussing use by former employee of information available on LinkedIn, Facebook, and Bloomberg to compile customer information comparable to former employer customer database, and concluding that ready availability of such information defeated trade secret claim); Complaint at 10, TEKSystems, Inc. v. Hammermick, 2010 WL 1624258 (D. Minn. Mar. 16, 2010) (No. 0:10-CV-00819) (alleging that former employees contacted former employer's customers via LinkedIn in violation of non-solicitation covenant in employment contract).

6. *Cf.* Yancy v. U.S. Airways, Inc., No. 10-983, 2011 WL 2945758, at *1 (E.D. La. July 20, 2011) (granting summary judgment in employee's sexual harassment suit based on Facebook posts by colleagues); Delfino v. Agilent Techs., Inc., 52 Cal. Rptr. 3d 376 (Cal. Ct. App. 2006) (resolving negligent and intentional infliction of emotional distress claims brought by victim of threatening e-mails and web bulletin board postings against employer after perpetrator used workplace computers); Tresa Baldas, *'Textual Harassment' on the Rise; Text Messages Can Prove to Be Potent Evidence in Bias Suits*, 30 NAT'L L.J., no. 46, 2009, at 1, 1 (discussing a $450,000 settlement paid by university after women's athletic coach harassed female players with text messages).

connections with coworkers, supervisors, customers, and vendors through social network sites like Facebook, Twitter, Instagram, and Pinterest, and she uses her employer-issued laptop or smartphone to access her social networks, to check her personal web-based e-mail, or to exchange personal text messages, among other things.[7]

The rapid evolution of workplace technologies raises a myriad of novel legal questions, and the law simply has not kept pace in providing answers.[8] Gone are the days when employer monitoring could be accomplished only by observing an employee's conduct at work, listening to her telephone conversations from across the room, or conducting a physical search of her desk or office.[9] Modern technologies permit employers to access not only any e-mail messages an employee sends or receives using her employer-provided account, but also any websites she visits while on the employer's network or equipment, including personal web-based e-mail accounts.[10] Further, with over 900 million people on Facebook,[11] chances are good that an employer can access a multitude of information there or on other social network sites, whether related to the company's business or the employee's work, or not.[12] Such a wealth of available information breeds ambiguity

---

7. *See Stengart*, 990 A.2d at 654–55 ("In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur.").

8. *See*, *e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (describing federal statutes addressing privacy rights in electronic and online information as "a complex, often convoluted, area of the law," noting that the statutes were enacted "prior to the advent of the Internet and the World Wide Web," and concluding that "the existing statutory framework is ill-suited to address modern forms of communication").

9. *Cf.* O'Connor v. Ortega, 480 U.S. 709, 712–14 (1987) (assessing an employer search of employee's desk and office in light of privacy concerns implicated by the Fourth Amendment); K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984) (evaluating invasion of privacy claim based on employer search of employee's workplace locker).

10. *See* Laura Petrecca, *More Employers Use Tech to Track Workers,* USA TODAY (Mar. 17, 2010, 12:51 AM), http://usatoday30.usatoday.com/money/workplace/2010-03-17-workplaceprivacy15_CV_N.htm ("Managers use technological advances to capture workers' computer keystrokes, monitor the websites they frequent, even track their whereabouts through GPS-enabled cellphones.").

11. FACEBOOK NEWSROOM, *supra* note 2.

12. *Cf.* Petrecca, *supra* note 10 ("Smarsh, one of many firms that offers technology to monitor, archive and search employee communications on

concerning the bounds of permissible employer access to, and use of, such information, and beckons for legal answers.

The law is far from silent on the topic of workplace privacy. The privacy rights of workers underlie lawsuits in the state and federal courts with increasing frequency,[13] while state legislatures grapple with striking an appropriate balance between employer prerogative and employee rights,[14] and the federal government considers various approaches it might take.[15] In addition, the debate surrounding workplace privacy

---

e-mail, IM, Twitter and text-messaging, services about 10,000 U.S. workplaces.").

13. *See, e.g.*, Nat'l Fed'n of Fed. Emps.-IAM v. Vilsack, 681 F.3d 483, 499 (D.C. Cir. 2012) (striking down policy of random drug testing of Forest Service Job Corps Center employees on grounds employer's stated need for such testing did not outweigh employees' privacy interests); Doe v. Luzerne Cnty., 660 F.3d 169, 175–78 (3d Cir. 2011) (holding that female deputy sheriff's constitutional invasion of privacy claims were viable under the Due Process Clause of the Fourteenth Amendment based on video surveillance of flea decontamination process, during which she was partially nude); Coughlin v. Town of Arlington, No. 10-10203-MLW, 2011 WL 6370932, at *1–2 (D. Mass. Dec. 19, 2011) (finding some privacy rights sufficient to support claims of school teacher and principal against school district and certain of its employees who accessed plaintiffs' work and personal e-mail accounts and disseminated messages therefrom in connection with investigation of alleged improper sexual relationship); Koeppel v. Speirs, 808 N.W.2d 177, 186 (Iowa 2011) (adopting expansive view of tort of invasion of privacy under which plaintiffs' claims of video surveillance in workplace bathroom survived summary judgment even though camera was inoperable at time of its discovery, because employer's electronic device "could have invaded privacy in some way").

14. *E.g.*, COLO. REV. STAT. § 24-72-204.5 (2008) (providing for notice by public employers of employee electronic monitoring); CONN. GEN. STAT. ANN. § 31-48d (West 2011) (mandating that employers provide prior written notice of electronic monitoring by employees); DEL. CODE ANN. tit. 19, § 705 (2005) (requiring employer notice to employees of electronic monitoring); TENN. CODE ANN. § 10-7-512 (2012) (requiring same); Kathy Lundy Springuel, *Maryland Is First State to Restrict Employer Demands for Employee, Applicant Passwords*, Human Resources Rep. (BNA), at A-12 (May 7, 2012) (identifying Maryland as first state to pass legislation restricting employer requests for employee and applicable social network passwords and noting that several other states have similar legislation pending).

15. *E.g.*, Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(b) (2012) (specifying when disclosure of employee records may be allowed by employers); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2012) (discussing the protection, obligations, disclosure, and enforcement of not-public personal information); USA PATRIOT Act, 18 U.S.C. § 1030 (2012) (discussing fraudulent and unauthorized access in connection with computers); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012) (discussing the different prohibited ramifications of intercepting and disclosing wire, oral, or electronic communications); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012) (discussing unlawful access to stored

issues has garnered the attention of numerous legal scholars who have published a plethora of books and articles exposing the topic.[16] Yet amidst all this banter, no clear consensus has emerged. Or, if there is a consensus, it is one of ambiguity.

Out of the abyss of uncertainty, however, a trend may be emerging. Early workplace technology cases were few and far between and evinced trepidation at confronting the novel issues.[17] This apparent trepidation seemed to manifest itself in reluctance to expand the privacy rights of workers, so that the cases nearly always resolved in the employer's favor.[18] But the

---

communications and the penalties associated therewith); E-Government Act of 2002, 44 U.S.C. § 36 (2006) (discussing the management and promotion of electronic government services); Wireless Communication and Public Safety Act of 1999, 47 U.S.C. § 222 (2006) (discussing telecommunications carriers' duty to protect the confidentiality of customers); PATRIOT Sunsets Extension Act of 2011, S. 1038, 112th Cong. (2011) (discussing intelligence and terrorism justifications for searching records).

16. *See generally* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW (3d ed. 2009) (analyzing privacy in the employment relationship and discussing relevant statutes and regulations); Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435 (2011) (describing harms posed by digital hate and proposing solutions); Althaf Marsoof, *Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression*, 19 INT'L J.L. & INFO. TECH. 110 (2011) (discussing developments in social networking and suggesting approaches to privacy-specific legislation); Christopher E. Parker, *The Rising Tide of Social Media*, FED. LAW., May 2011, at 14 (discussing implications of social media use in the workplace); Marie-Andrée Weiss, *The Use of Social Media Sites Data by Business Organizations in Their Relationship with Employees*, J. INTERNET L., Aug. 2011, at 16 (examining the pitfalls of using social media sites in decisions relating to hiring, maintaining, and terminating employment).

17. *Cf.* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 886 (9th Cir. 2002) (affirming summary judgment for employer because employer did not "intercept" employee's communications within meaning of Wiretap Act simply by accessing employee's secure bulletin board).

18. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2003) (concluding that employer accessing employee e-mail stored on company's central file servers without permission did not violate Electronic Communications Privacy Act because employer owned the servers); Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002) (holding that employees had no reasonable expectation of privacy in work e-mail and that employer had legitimate business interest in guarding the workplace against offensive communications); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (dismissing employee's claim on grounds employee could not establish a reasonable expectation of privacy nor highly offensive invasion based on employer's interception of e-mail messages sent from employee's home computer through company e-mail system, notwithstanding employer's assurances that e-mail would not be intercepted); *see also infra* Part II

tide may be turning. Though some courts remain wary of entering the fray today, others are now tackling the issues head on, and a relative flurry of recent activity may suggest a trend in the opposite direction.[19] This Article delves deeply into this recent flurry and juxtaposes it against early workplace technology law to expose the shifting trend. Further, it does so in novel ways. While many scholars have opined about the rights of workers and the needs of employers in light of emerging technologies,[20] this is the first scholarly work to

---

(discussing early technology cases and consensus in favor of employer prerogative over employee privacy). In 2001, one commentator starkly exposed this phenomenon by offering that "the employee's right of privacy is a hollow shell against the lead weight of the employer's claim to run his business as he pleases." Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMP. RTS. & EMP. POL'Y J. 453, 475 (2001).

19. *Cf.* City of Ontario v. Quon, 560 U.S. 746, 756–60 (2010) (upholding public employer's search of text messages sent from and received on employee's employer-issued paging device, assuming without deciding that employee had reasonable expectation of privacy but concluding that employer's search was reasonable); Steinbach v. Vill. of Forest Park, No. 06 C 4215, 2009 WL 2605283, at *5 (N.D. Ill. Aug. 25, 2009) (denying employer's motion to dismiss intrusion upon seclusion claim brought after employer searched plaintiff-employee's work e-mail account because the defense based on allegation of provider exemption under Stored Communications Act did not apply given that third party, rather than employer, provided e-mail service); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556, 571 (S.D.N.Y. 2008) (finding unlawful employer's search of employee e-mail account even though accessed on employer's equipment because account was maintained by third-party provider rather than employer and employee therefore established reasonable expectation of privacy in such account); *see also infra* Part II.A (discussing recent technology cases reflective of a trend toward employee privacy rights).

20. *See, e.g.*, Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 325–28 (2011) (proposing a notice requirement and substantive restrictions in workplace monitoring policies); Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011) (comparing worker privacy in Europe and the United States); Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331, 340–90 (2010) [hereinafter Levinson, *Carpe Diem*] (proposing legislation to protect employee privacy rights); Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609, 620–21 (2009) [hereinafter Levinson, *Industrial Justice*] (positing that no systematic statutory scheme currently guides common law development of employee privacy rights); Lindsay Noyce, *Private Ordering of Employee Privacy: Protecting Employees' Expectations of Privacy with Implied-in-Fact Contract Rights*, 1 AM. U. J. LAB. & EMP. L.F. 27 (2011) (discussing evolution of employee privacy rights in light of changing technology and advocating for protection of employee privacy under implied-in-fact contract theory); Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United*

conduct a comprehensive analysis of ultra-recent developments in the technology-based privacy rights of workers, and the only to suggest a trend toward employee rights emerging from them.[21]

This Article proceeds in three Parts. Part I surveys what are termed here the "early" workplace technology privacy laws, examining initial forays into the field by courts and legislatures surrounding the turn of the new millennium, and attempting to extract from those laws a theme favoring employer prerogative, rooted in apprehension.[22] Part II then fast forwards a decade or more, examining more recent developments in workplace technology laws, which stand in stark contrast to the reluctant entries of the preceding era.[23] Including discussion of case law, statutes, administrative decisions, and position statements, this Part offers a comprehensive look at modern-era regulation of technology-based privacy concerns in the workplace, revealing a shifting paradigm away from employer prerogative

---

States and Its De-evolution for American Employees, 42 J. MARSHALL L. REV. 83 (2008) (arguing that employee privacy rights are diminishing and that employer access to personal employee information is extending beyond workplace into employee homes).

21. Much of the scholarly literature addressing workplace privacy in modern technologies tackles the myriad implications for discovery, assuming the eventual advent of litigation. *See, e.g.*, Louise L. Hill, *Gone But Not Forgotten: When Privacy, Policy and Privilege Collide*, 9 NW. J. TECH. & INTELL. PROP. 565 (2011) (examining employee privacy expectations as relevant to application of attorney-client privilege when communications are made over employer network or equipment). Other scholars lament the absence or insufficiency of the current law to afford adequate protection to employees. Levinson, *Carpe Diem, supra* note 20, at 331 ("Scholars generally agree that the law in the United States fails to adequately protect employees from technological monitoring."); Levinson, *Industrial Justice*, *supra* note 20, at 620–21 (lamenting the absence of statutory protection for employee privacy in workplace technologies); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357 (2006) ("Currently, the privacy protections in the United States are riddled with gaps and weak spots."). Still others suggest, quite contrary to this Article, that employee privacy rights are actually diminishing. Sprague, *supra* note 20, at 89 (positing that "the current right to privacy in the United States [is] contextual, fluid, and easily subject to elimination"). A few recognize the pro-employee trend that this Article posits, but take a different approach. *See, e.g.*, Michael Z. Green, *Against Dumpster-Diving for Email*, 64 S.C. L. REV. 323, 348–62 (2012) (suggesting that employee privacy rights in workplace technologies may be expanding, but focusing on cases and other legal developments specific to application of attorney-client privilege). As such, this is the first scholarly work to both take a comprehensive comparative approach and suggest a trend toward employee rights.

22. *See infra* Part I.

23. *See infra* Part II.

in favor of employee rights. Part III then juxtaposes the early laws of Part I against the recent developments of Part II, offering explication of the apparent evolution, proposing lessons to be gleaned from the development of the law, and hypothesizing about potential next steps.[24]

I. EARLY FORAYS INTO WORKPLACE PRIVACY IN LIGHT OF EMERGING TECHNOLOGIES

The pioneer plaintiffs in workplace privacy cases involving emerging technologies like e-mail and the Internet faced an uphill battle, attempting to establish new rights in unfamiliar territory. In an effort to give the appearance of credibility to their otherwise novel claims, many of these trailblazing plaintiffs pirated the causes of action commonly relied upon by aggrieved employees and manipulated them to suit the evolving circumstances. The absence of directly applicable laws—whether judge-made or the product of state or federal legislative reform—necessitates such an approach. Common-law tort claims such as invasion of privacy and intrusion upon seclusion, as well as the tried-though-rarely-true wrongful discharge in violation of public policy, were therefore prime suspects for the escapades of some early litigants. Others, meanwhile, attempted to fashion viable claims out of statutes addressed more directly to privacy in technology but not necessarily adequate for the employment setting. Notably, and as explained more fully below, in none of these cases were the pioneering plaintiffs particularly successful.

A. THE EARLY COMMON-LAW CASES

1. A Firm Foundation of Disdain for Privacy Rights

The earliest forays into the domain of employee privacy rights in emerging technologies date back to the early 1990s,[25] when e-mail itself was in its relative infancy.[26] Perhaps

---

24. *See infra* Part III.

25. *See* John D. Blackburn et al., *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*, 6 DEPAUL BUS. L.J. 41, 42 (1993) ("Advanced technology in sophisticated information systems . . . contribute[s] to a continuing concern about privacy in the workplace.").

26. *See The 41-Year History of Email,* MASHABLE (Sept. 20, 2012), http://mashable.com/2012/09/20/evolution-email/ (discussing how internet service providers allowed widespread access to the internet in 1991, but there were still limited options).

reflective of the trepidation with which the courts entered the fray, one of the earliest decisions addressing employee privacy claims related to technological monitoring, *Bourke v. Nissan Motor Corp.*, was never published and thus is not widely available.[27] In that case, the court's swift rejection of the plaintiffs' claims starkly illustrates the court's distaste for the suggestion that such privacy rights should exist.[28] The plaintiffs, Bonita Bourke and Rhonda Hall, worked for Nissan Motor Corp. as Information Systems Specialists tasked primarily with troubleshooting for personnel who used the central computer system at Infiniti dealerships.[29] After random discovery of an e-mail message sent by Bourke to a dealership employee, which was of a personal, sexual nature, Nissan conducted a further review of Bourke's e-mail and found "substantial numbers of personal, including sexual, messages from Bourke" as well as her co-plaintiff Hall.[30] The subject e-mail messages violated Nissan's policy prohibiting personal use of the company computer system, so Nissan issued disciplinary warnings to both Bourke and Hall as a result of its discovery.[31] Subsequently, both plaintiffs received poor performance reviews.[32] Nissan then issued Bourke a final disciplinary warning when her performance continued to suffer, but she resigned the day after receiving it.[33] The company terminated Hall's employment the same day.[34]

Shortly after leaving Nissan, Bourke and Hall joined as plaintiffs in a suit against the company, claiming that Nissan's review of their e-mail accounts constituted a common-law invasion of privacy, violated their constitutional right to privacy as well as criminal wiretapping and eavesdropping statutes, and gave rise to a claim for wrongful discharge in

---

27. *See* Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html. The decision does not appear in either of the primary legal databases, Westlaw or LexisNexis, but it has a dedicated page on Wikipedia. *See Bourke v. Nissan Motor Co.*, WIKIPEDIA, http://en.wikipedia.org/wiki/Bourke_v._Nissan_Motor_Co. (last updated Nov. 8, 2013).

28. *Cf. Bourke*, No. B068705.

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

violation of public policy.[35] The trial court granted Nissan's motion for summary judgment, refusing to recognize any reasonable expectation of privacy in workplace e-mail, and plaintiffs appealed.[36] The plaintiffs fared no better at the appellate level, though.[37] Addressing first the plaintiffs' claims that Nissan violated privacy rights protected by both the common law and the Constitution, the court gave short shrift to the plaintiffs' allegations, finding that the company's computer policy permitting only business use, coupled with the plaintiffs' knowledge that Nissan employees other than the intended recipient could review e-mail messages, negated any objectively reasonable expectation of privacy in them.[38] In the absence of any such reasonable expectation, their privacy claims failed.[39]

The plaintiffs' remaining claims fared no better.[40] Both of the statutory causes of action failed on the grounds that neither statute invoked by the plaintiffs addressed interception of e-mail.[41] Instead, both were addressed to communication modes like telegraphs and telephone wires that existed at a time when no one even contemplated the eventual invention now known as electronic mail.[42] And, the plaintiffs' claims of wrongful discharge in violation of public policy likewise failed to pass muster, as the absence of a constitutional right to privacy in the e-mail, announced earlier in the court's opinion, obviated its demise—without a public policy violation, no wrongful discharge could have occurred.[43] Thus, in this very early clash between employee privacy rights and workplace technologies, the prerogative of the employer to control its workplace easily prevailed.

Another three years would pass after the decision in *Bourke* before the case that became widely known as the first published opinion addressing employee privacy rights in e-mail would appear.[44] That case was *Smyth v. Pillsbury Co.*, rendered

---

35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.* (discussing California Penal Code sections 631 and 632).
43. *Id.*
44. *Cf.* Charles J. Muhl, *Workplace E-mail and Internet Use: Employees and Employers Beware*, MONTHLY LAB. REV., Feb. 2003, at 36, 37 ("Employees often mistakenly believe that their use of the Internet and e-mail at the

in 1996, and, like *Bourke*, it also followed the common-law route.[45] Plaintiff-employee Smyth, relying upon his employer's repeated assurances that all e-mail communications would remain confidential and could not supply grounds for termination, exchanged several e-mail messages with his supervisor that the company contends derided management.[46] Notwithstanding its clear policy to the contrary, Pillsbury terminated Smyth's employment on the basis of the "inappropriate and unprofessional comments" made in the e-mail messages.[47] Smyth then brought a diversity lawsuit in Pennsylvania federal court seeking relief under the traditional employment tort of wrongful discharge in violation of public policy.[48] Without even filing an answer, Pillsbury responded with a motion to dismiss for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6).[49]

The court granted the employer's motion to dismiss only four months after the complaint was filed and without any other proceedings taking place.[50] Its discussion of the law began with a caution-ridden exposition of the tort's narrow scope.[51] In Pennsylvania, as in many or indeed most of the forty-nine states in which the at-will doctrine persists,[52] erosions of the employer's ability to discharge an employee for any reason remain narrow.[53] The court explained that

---

workplace is private when, in fact, courts have found no reasonable expectation of privacy in such use and have consistently permitted employers to monitor and review activity. The seminal case in this area is *Smyth v. The Pillsbury Company* . . . .").

45. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). As evidence of the Eastern District of Pennsylvania's role as seminal, the court in *Garrity v. John Hancock Mutual Life Insurance Co.* referenced "a dearth of case law on privacy issues with regard to office email," then cited *Smyth* as "instructive." Garrity v. John Hancock Mut. Life Ins. Co., No. Civ.A. 00-12143-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002).

46. *Smyth*, 914 F. Supp. at 98–99.

47. *Id.* at 98.

48. *Id.* at 99.

49. *Id.* at 98; Docket, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (No. 95-CV-05712).

50. Docket, *supra* note 49.

51. *Smyth*, 914 F. Supp. at 99.

52. *See generally* Miriam A. Cherry, *A Taxonomy of Virtual Work*, 45 GA. L. REV. 951, 986 n.159 (2011) ("The at-will rule is that an employee may be fired for a good reason, a bad reason, or no reason at all . . . . The at-will rule is the law in forty-nine states with Montana the sole exception.").

53. *See Smyth*, 914 F. Supp. at 99 ("Pennsylvania is an employment at-will jurisdiction and an employer may discharge an employee with or without

Pennsylvania law recognizes exceptions to the at-will doctrine only "in the most limited of circumstances, . . . where discharge of an at-will employee threatens or violates a clear mandate of public policy," cautioning that the "exception is an especially narrow one."[54] Specifically, Pennsylvania courts had recognized the tort in only three limited circumstances: when an employee is discharged for serving on jury duty, when an employer refuses hire based on a prior conviction, and when an employee is fired for proper reporting of federal-regulation violations.[55] In each circumstance, the court that rendered the decision relied directly and heavily upon a clearly defined and firmly established public policy, embodied in legislation, judicial decisions, or administrative rules or regulations.[56] Thus, the

---

cause, at pleasure, unless restrained by some contract." (internal quotation marks omitted)).

54. *Id.*

55. *Id.*

56. *Id.* In the case of jury duty, the rendering court cited the Pennsylvania Constitution and state statutes referencing "the necessity of having citizens freely available for jury service." *Id.* (quoting Reuther v. Fowler & Williams, Inc., 386 A.2d 119, 121 (Pa. Super. Ct. 1978)). As to use of prior convictions in hiring, the court that issued the decision cited the state constitution and judicial decisions reflecting "'the deeply ingrained public policy of this State . . . to avoid unwarranted stigmatization of and unreasonable restrictions upon former offenders.'" *Id.* (quoting Hunter v. Port Auth. of Allegheny Cnty., 419 A.2d 631, 636 n.5 (Pa. Super. Ct. 1980)). Finally, as to reporting violations of federal regulations, the rendering court relied upon policies typically supporting whistleblower protections, including that the pertinent law required the employee to report the violations, that the employee possessed relevant knowledge and expertise to inform his report, and that the employee did not bypass any internal reporting procedures. *Id.* (citing Field v. Phila. Elec. Co., 565 A.2d 1170, 1180 (Pa. Super. Ct. 1989)). "Whistleblower" is the term commonly used to refer to an employee who reports unlawful activity by his employer. *See Whistleblower Definition*, WIKIPEDIA, http://en.wikipedia.org/wiki/Whistleblowing (last visited Feb. 7, 2014) ("A whistleblower (whistle-blower or whistle blower) is a person who exposes misconduct, alleged dishonest or illegal activity occurring in an organization." (footnote omitted)). Whistleblower protection laws have flourished in recent years, particularly in the wake of the Enron and Worldcom debacles which were brought to light by corporate whistleblowers. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (providing civil private right of action and remedy for whistleblowers who report violations of various securities laws, among other things); Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 1558, 124 Stat. 119, 261 (2010) (codified at 29 U.S.C. § 218C (2012)) (providing broad protection from retaliation for employees who report violations of the Act's provisions); American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 1553, 123 Stat. 115, 297 (2009) (prohibiting any private employer or state or local government entity receiving funds under the Act from retaliating against employees who disclose information concerning

court made plain that the applicable law recognizes a viable claim only when the public policy allegedly violated by the employee's discharge is clearly defined in a firmly established law.[57]

Because Smyth's claim fit into none of the pigeonholes established under Pennsylvania law—his claim had nothing to do with jury duty, a prior conviction, or whistleblowing[58]—he faced a substantial uphill battle. Attempting to convince the court to drill a new pigeonhole, Smyth contended that his discharge violated the state's public policy favoring an employee's right to privacy, as reflected in common law.[59] He relied upon a decision from the United States Court of Appeals for the Third Circuit, *Borse v. Piece Goods Shop, Inc.*,[60] in which the plaintiff-employee claimed wrongful discharge upon her refusal to submit to a urinalysis and a search of her personal property at work.[61] *Borse*, like *Smyth*, was also in federal court on the basis of diversity jurisdiction.[62] The *Borse* court therefore searched Pennsylvania law for instruction on whether the courts of that state would recognize a claim for wrongful discharge in violation of public policy on the basis of an invasion of privacy.[63] Finding no binding state law on point, the Third Circuit engaged in an "*Erie* guess"—an informed

---

improper use of stimulus funds); Consumer Product Safety Improvement Act of 2008, Pub. L. No. 110-314, § 219, 122 Stat. 3016, 3062 (prohibiting retaliation against employees who provide information about violations of the Act to his or her employer, to the federal government, or to the attorney general of any state); Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 806, 116 Stat. 745, 802 (codified at 18 U.S.C. § 1514A (2012)) (making unlawful retaliation by publicly held companies against whistleblower employees who make certain covered disclosures).

57. *See Smyth*, 914 F. Supp. at 101 ("[D]efendant's actions did not tortiously invade the plaintiff's privacy and, therefore, did not violate public policy.").

58. *See id.* at 100.

59. *Id.*

60. 963 F.2d 611 (3d Cir. 1992).

61. *Smyth*, 914 F. Supp. at 100.

62. *See id.* (discussing the Third Circuit's application of Pennsylvania law, which occurs only in diversity cases); *see also* 28 U.S.C. § 1332 (2012) (providing for jurisdiction in federal courts over state-law claims on the basis of diversity of citizenship); *Borse*, 963 F.2d at 613 ("The district court's subject-matter jurisdiction was based on diversity of citizenship pursuant to 28 U.S.C. § 1332 . . . . Federal courts sitting in diversity must apply the substantive law of the state whose laws govern the action.").

63. *Borse*, 963 F.2d at 621–22.

supposition about what the Pennsylvania Supreme Court would decide *if* it were faced with a comparable situation.[64]

The court in *Borse* concluded that the Pennsylvania Supreme Court might recognize a claim of wrongful discharge in violation of public policy based on invasion of privacy, but only if the alleged invasion was "substantial and highly offensive."[65] Further, the court projected that in determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, "Pennsylvania would adopt a balancing test which balances the employee's privacy interest against the employer's interest in maintaining a drug-free workplace."[66] Having announced those principles of law, though, the *Borse* court then remanded, with instructions that the district court grant the plaintiff leave to amend so that she might allege specifically how her employer's actions violated her right to privacy.[67] Thus, while the *Borse* decision offered Smyth some grounds upon which to rest his contention that his claim was viable, it lacked any specific instruction as to how the court's hypothesized standard might apply.[68]

The *Smyth* court did not question the reliability of the *Borse* court's crafted rules, or, more generally, that the law of Pennsylvania would recognize the tort of wrongful discharge based on violation of the public policy favoring employee privacy.[69] Nevertheless, the court concluded that Smyth failed to state a claim upon which relief could be granted.[70] The central fallacy in Smyth's claim, according to the court, was a broad proposition of law that wields especially significant

---

64. *Id.* at 625 ("[W]e predict that the Pennsylvania Supreme Court would apply a balancing test to determine whether the Shop's drug and alcohol program . . . invaded Borse's privacy."). The term "*Erie* guess" refers to the Supreme Court's seminal decision in *Erie Railroad Co. v. Tompkins*, which held that state substantive law applies in federal courts sitting in diversity. *See* Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938). When there is no state law on point, the federal court is forced to guess how the highest court of that state *would* decide the issue, if it were presented. Travelers Cas. & Sur. Co. of Am. v. Ernst & Young LLP, 542 F.3d 475, 482–83 (5th Cir. 2008) ("When state law provides no definitive answers to the question presented, we must make an educated '*Erie* guess' as to how the [state] Supreme Court would resolve the issue.").

65. *Borse*, 963 F.2d at 621.

66. *Smyth*, 914 F. Supp. at 100 (citing *Borse*, 963 F.2d at 625).

67. *Id.* (citing *Borse*, 963 F.2d at 626).

68. *See id.*

69. *Id.* at 101.

70. *Id.* at 100–01.

weight here—that an employee lacks "a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system."[71] Perhaps even more importantly, the court boldly declared this so, "notwithstanding any assurances that such communications would not be intercepted by management."[72] Then, further entrenching its cool reception to any suggestion of privacy in e-mail, the court distinguished the e-mail context of Smyth's case from the urinalysis exam at issue in *Borse*: "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 the company e-mail system. We find no privacy interests in such communications."[73] Thus, the court, seemingly without the least hesitation, declared quite unequivocally that employees should expect no privacy in workplace e-mail communications.

The court's stark scorn for any claimed privacy in workplace electronic communications did not end there, however. The court went on to declare that even if a reasonable expectation of privacy could be found (and although here it could not), a reasonable person could not consider the interception of Smyth's e-mail communications "to be a substantial and highly offensive invasion of . . . privacy."[74] Again the court relied upon the distinction it perceived between urinalysis and physical searches of personal property, on one hand, and review of e-mail communications, on the other.[75] The court justified its conclusion in light of the policy favoring employer control: "Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[76] Thus, the court unwaveringly declined to recognize any employee privacy interest in e-mail communications sent on the company

71. *Id.* at 101.
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*

system, notwithstanding a published policy statement to the contrary.[77] Employer prerogative reigned supreme.

The palpable malevolence for employee privacy expressed by the *Smyth* court is remarkable, but the impact of its holding is confounded by the procedural posture. The court decided the case on a motion to dismiss filed even before an answer to the complaint.[78] The essence of such motions is that the plaintiff's complaint fails to state an actionable claim so that, under the standard that governed at the time, the motion could be granted only if the court concluded that plaintiff could prove "no set of facts" that would support his claim for relief.[79] The standard was quite forgiving, and resulted in dismissal only when the complaint revealed that the claims were indubitably defective, regardless of any then-unknown facts a plaintiff might conceivably muster in support.[80] The precedential effect

---

77. *See id.*

78. *Id.* at 98; Docket, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (No. 95-CV-05712).

79. Conley v. Gibson, 355 U.S. 41, 45 (1957). As any litigator, proceduralist, or even first-year law student undoubtedly knows, the United States Supreme Court in recent years rendered two seminal decisions addressing the standard governing such motions under Federal Rule of Civil Procedure 12(b)(6). *See* Ashcroft v. Iqbal, 556 U.S. 662 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007). While some debate lingers among the courts and commentators as to whether, and if so, to what extent, *Twombly* and *Iqbal* altered the standard under Rule 12(b)(6), it is generally accepted that the Court "retired" the *Conley* "no set of facts" standard in favor of a "plausibility" standard and that, at a minimum, it is possible for a court to interpret and apply that plausibility standard in such a way that might lead to dismissal of some cases that would have survived under *Conley*. *See Iqbal*, 556 U.S. at 670 (describing *Twombly*'s effect as retirement of *Conley's* pleading standard); *Twombly*, 550 U.S. at 563 (stating that *Conley*'s "no set of facts" standard "has earned its retirement"); JOE S. CECIL ET AL., FED. JUDICIAL CTR., MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM AFTER *IQBAL* (2011), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/motioniqbal.pdf/$file/motioniqbal.pdf (reviewing empirical data concerning motions to dismiss filed before and after *Twombly* and *Iqbal*, and concluding that no statistically significant change occurred in how motions were resolved before those decisions as compared to after).

80. *E.g.*, Arthur R. Miller, *From* Conley *to* Twombly *to* Iqbal*: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 6, 18 n.60 (2010) (explaining development of pleadings law and indicating that dismissal became more likely under *Twombly* and *Iqbal* than it had been under *Conley*); A. Benjamin Spencer, *Plausibility Pleading*, 49 B.C. L. REV. 431, 434–35 (2008) (describing the pleading regime under *Conley* as "simplified" and as more permissive to plaintiffs than under the modernized standard); Michael C. Dorf, *Should Congress Change the Standard for Dismissing a Federal Lawsuit?*, FINDLAW (July 29, 2009), http://writ.news.findlaw.com/dorf/20090729.html ("*Twombly* and *Iqbal* make it harder for plaintiffs who might

of such decisions was significant because the holding indicated not just that the plaintiff in that particular case could not muster sufficient proof of his claims, but rather could be read more broadly to stand for the proposition that the law would not recognize a claim in any such comparable case. The import of *Smyth* as the trailblazing opinion addressing privacy in workplace technologies[81] was therefore salient: a plaintiff lacks any reasonable expectation of privacy in workplace e-mail communications, even if the employer expressly guarantees otherwise, and the employer's enforcement of its rights to monitor employee e-mail cannot support a claim for relief by an aggrieved employee.[82]

2. In *Smyth*'s Wake

On the heels of *Smyth*, other courts confronting common-law claims that arose from monitoring of workplace technologies followed the *Smyth* court's lead.[83] *McLaren v. Microsoft Corp.* is archetypal and mirrors *Smyth* in myriad respects.[84] Plaintiff Bill McLaren worked for Microsoft Corporation in Texas.[85] He worked in an office environment, and Microsoft furnished him with a networked computer and e-mail address.[86] When another employee accused McLaren of sexual harassment, Microsoft suspended McLaren's employment pending an investigation into the accusations.[87] In response, McLaren requested access to his e-mail in an effort to disprove the allegations, but Microsoft refused general access,

---

have meritorious cases, but need access to defense witnesses and files, to have their cases heard.").

81. Unpublished decisions entered prior to *Smyth* reached conclusions consistent with it. *See, e.g.*, Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html (holding that plaintiff employees had no objectively reasonable expectation of privacy in e-mail messages sent on company computer system despite employees' subjective belief to the contrary due to fact that access was limited by password). The *Bourke* decision is particularly notable because the right to privacy of California citizens is firmly rooted in an amendment to that state's constitution. *See* CAL. CONST. art. I, § 1.

82. *See Smyth*, 914 F. Supp. at 100–01.

83. *See, e.g.*, Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999).

84. *See McLaren*, 1999 WL 339015.

85. *Id.* at *1.

86. *Id.*

87. *Id.*

instead requiring that he specify to company officials the identity and location of individual messages he wished to see.[88] He never made any such request, and Microsoft terminated his employment shortly thereafter.[89]

McLaren filed suit in Texas state court claiming an invasion of privacy by Microsoft when it accessed e-mail messages stored in "personal folders" on his work computer and subsequently disclosed the contents of those messages to "third parties."[90] McLaren contended that he manifested a reasonable expectation of privacy in e-mail messages stored in those "personal folders" because Microsoft's system enabled him to create a password to restrict access to those folders, and he took advantage of that technology.[91] In response, Microsoft filed, *inter alia*, a motion to dismiss for failure to state a claim upon which relief could be granted.[92] The trial court granted Microsoft's motion, and McLaren appealed.[93]

The analysis of the Texas Court of Appeals in *McLaren* bears striking similarities to that of the federal district court in *Smyth*.[94] After finding no merit in McLaren's preliminary procedural objection, the court proceeded to conclude, just as the court in *Smyth* did, that the plaintiff's invasion of privacy claim must fail as a matter of law because he had no reasonable expectation of privacy in his e-mail messages, and, even if he did, Microsoft's review of them would not have been highly offensive to a reasonable person.[95] A key component of McLaren's privacy argument rested upon the password-

88. *Id.*

89. *Id.*

90. *Id.*

91. *Cf. id.* ("McLaren allege[d] . . . that [b]y allowing [him] to have a personal store password for his personal folders, [McLaren] manifested and [Microsoft] recognized an expectation that the personal folders would be free from intrusion and interference." (internal quotation marks omitted)).

92. *Id.* The Texas Court of Appeals referred to Microsoft's response as a "special exception," but its description of the procedural device indicates that it is comparable to a motion to dismiss for failure to state a claim upon which relief can be granted under Federal Rule of Civil Procedure 12(b)(6). *Id.* at *2 (describing a special exception under Texas procedural rules).

93. *Id.* at *2.

94. *See supra* Part I.A.1 (discussing Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996)).

95. *McLaren*, 1999 WL 339015, at *2, *4–5. The court concluded that "a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion." *Id.* at *5.

protection afforded to his e-mail messages by Microsoft.[96] The e-mail system that Microsoft utilized allowed McLaren to restrict access to his personal e-mail folders with a "personal store" password created by him.[97] This password afforded additional protection beyond the network password that McLaren used to access the Microsoft network.[98] McLaren contended that by allowing him to protect his personal folders with a password known only by him, Microsoft should have known that McLaren expected privacy in messages stored there—privacy that Microsoft invaded when it decrypted his personal store password and accessed his folders.[99]

In support of his contention that the personal store password gave rise to a reasonable expectation of privacy, McLaren relied principally on an invasion of privacy case that arose in a more traditional setting.[100] In *K-Mart Corp. v. Trotti*, the plaintiff-employee claimed invasion of privacy when K-Mart searched the locker provided for her use at work.[101] The Texas Court of Appeals held that, even though the locker was the employer's property and would be subject to legitimate searches while unlocked, the "employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference" solely because, with the employer's knowledge, the employee provided her own lock.[102] McLaren argued that the password he created to protect the contents of his personal folders was directly analogous to the employee-provided lock in *Trotti*, and should likewise dictate a finding that his expectation of privacy was reasonable.[103]

The court disagreed with McLaren's suggestion, coolly rejecting the opportunity to import traditional privacy protections into the modern workplace.[104] As a threshold matter, the court distinguished Trotti's locker, provided solely for personal use, from McLaren's e-mail, which was integral to

---

96. *Id.* at *4.
97. *Id.* at *1.
98. *Id.*
99. *Id.*
100. *Id.* at *4.
101. 677 S.W.2d 632 (Tex. App. 1984).
102. *Id.* at 637.
103. *See McLaren*, 1999 WL 339015, at *4.
104. *See id.*

his work.[105] Reasoning that "the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment," the court rejected McLaren's argument that "only the technology is different."[106] K-Mart provided Trotti's locker solely for storage of her personal belongings, but Microsoft provided McLaren's computer and e-mail to enable him to perform his job.[107]

In a similar vein, the court also distinguished McLaren's case from Trotti's on grounds that her locker "was a discrete, physical place where the employee, separate and apart from other employees, could store her tangible, personal belongings."[108] By contrast, even those messages stored in McLaren's personal folders only ended up there after passing through the employer's network where they were fully accessible by Microsoft officials.[109] The crux of the court's rationale here seemed to be that because Trotti did not use the locker for any work-related purpose and stored only personal belongings there, its physical separation from the employer's property supported a viable expectation of privacy. McLaren, on the other hand, lacked any such reasonable expectation because the e-mail system on which he stored his "personal" messages also contained work-related messages, albeit in different locations.[110] The folders containing personal messages, according to the court, were not "discrete" in the way that Trotti's locker was, and thus warranted different treatment.[111] In the end, the employer's prerogative to monitor and search the employee's use of workplace technologies, notwithstanding their "personal" label, prevailed.[112]

The turn of the new millennium did not usher in much change in the approach courts took toward the privacy rights of employees in workplace technologies. The United States District Court for the District of Massachusetts, deciding

105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.* (noting that e-mail was provided so employees could perform job-related functions).
111. *See id.* (noting that the messages were initially transmitted over the company network).
112. *See id.*

Garrity v. John Hancock Mutual Life Insurance Co., continued the trend of rejecting common-law claims begun by the *Smyth* and *McLaren* courts, citing both as definitive authorities for the proposition that an employee has no reasonable expectation of privacy in e-mail messages transmitted via an employer's network.[113] The plaintiffs Nancy Garrity and Joanne Clark sued defendant John Hancock Mutual Life Insurance Company ("Hancock") when Hancock terminated their employment after discovering that both plaintiff-employees had transmitted numerous sexually explicit e-mail messages, many from internet joke sites, over the company's e-mail system.[114] Hancock contended that their conduct violated its e-mail policy, which prohibited "sexually oriented" messages and threatened disciplinary action for "inappropriate use of E-mail."[115] The policy also reserved Hancock's rights to review e-mail, albeit while indicating that such review would not occur with regularity: "All information stored, transmitted, received or contained in the company's E-mail systems is the property of John Hancock. It is not company policy to intentionally inspect E-mail usage. However, there may be business or legal situations that necessitate company review of E-mail messages and other documents."[116]

After Hancock terminated the plaintiffs' employment based on its perception that the plaintiffs had violated the company e-mail policy, plaintiffs sued, asserting, among other things, claims for invasion of privacy, violation of the Massachusetts Wiretap Act,[117] and wrongful discharge in violation of public policy.[118] Hancock filed a motion for summary judgment, which the court swiftly granted, offering only short explanations for the dismissal of each claim.[119] First, the court flatly rejected the plaintiffs' contention that the company's provision of password-protected personal e-mail folders gave rise to a reasonable expectation of privacy in the e-mail messages those folders contained.[120] Citing *Smyth* as instructive and adopting

---

113. Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002).

114. *Id.* at *1.

115. *Id.*

116. *Id.*

117. MASS. GEN. LAWS ch. 272, § 99 (1998).

118. *Garrity*, 2002 WL 974676, at *1.

119. *Id.* at *1–4.

120. *Id.* at *1–2.

wholesale the rationale offered in *McLaren*, the court reasoned that the plaintiffs' privacy expectations were unreasonable, notwithstanding the opportunity to create password-protected folders, because all messages contained in those folders had first to pass through the employer's network.[121] Further, the court went on to state that even if plaintiffs had some reasonable privacy expectations, the employer's "legitimate business interest in protecting its employees from harassment in the workplace would likely trump [those] privacy interests."[122] As such, plaintiffs' invasion of privacy claim failed.[123]

The *Garrity* plaintiffs were no more successful on their remaining claims.[124] First, as to their statutory claim under the Massachusetts Wiretap Act, the court concluded, with little explanation, that the communications at issue fell outside the scope of the statute's protection because "the reading of e-mails, after they have been transmitted to the recipient, does not constitute 'interception' within the wiretap statute."[125] The statute, which was originally enacted in an effort to redress wiretapping and eavesdropping in organized crime, pre-dated the inception and spread of e-mail by several decades.[126] As such, the statute is ill-equipped to address modern needs. Moreover, Massachusetts courts had already, prior to the decision in *Garrity*, interpreted the statute in such a way as to exclude e-mail messages stored in application or network folders because the reading of stored messages does not constitute "interception,"[127]—the act that the statute

---

121. *Id.* at *2 (citing McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. May 28, 1999)).

122. *Id.*

123. *Id.*

124. *Id.* at *3–4.

125. *Id.* at *3 (citing MASS. GEN. LAWS ch. 272, § 99 (1998)).

126. *See* MASS. GEN. LAWS ch. 272, § 99(A) ("The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety.").

127. *Id.* (defining interception as "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device"); *see* Mark E. Schreiber, *Employer E-mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 86 (2000) ("One can expect further interpretations of this state's wiretap statute to exclude from liability employer e-mail or Internet monitoring efforts, provided such systems have a demonstrable business purpose.").

prohibits.[128] Second, their wrongful discharge tort claim likewise failed, on grounds that it was duplicative of the invasion-of-privacy and statutory claims and thus effectively fell to preemption.[129] And, finding no greater success on their remaining claims—one under the Employee Retirement Income Security Act (ERISA) and one for defamation, neither of which is especially relevant here—the plaintiffs' case was dismissed in its entirety.[130] Thus, the *Garrity* plaintiffs, like those who came before them in *Bourke*, *Smyth*, and *McLaren*, garnered little sympathy for their alleged privacy violations, as the court in each case swiftly rejected the efforts of every plaintiff to carve out even a sliver of asylum in the abyss of cyberspace.

B. EARLY STATUTORY CLAIMS

Trailblazing plaintiffs aggrieved by workplace technology searches that they perceived as unfair and improper looked not only to the common law, but also to state and federal statutes, in an effort to find a remedy.[131] For the most part, they met no warmer reception on their statutory claims than their common-law ones, though. The statutes, like the common law, pre-dated the advent and spread of e-mail and the internet, and were therefore ill-suited to redress the wrongs that the plaintiffs alleged. Moreover, the judges who were deciding their claims faced a new frontier, attempting to apply antiquated legal regimes to complex and rapidly evolving technologies, with which many of them were mostly or even wholly unfamiliar.[132] The result was near wholesale rejection of the pioneer plaintiffs' efforts to find relief via statute, often as readily and swiftly as the courts had rejected their common-law claims.[133]

---

128. MASS. GEN. LAWS ch. 272, § 99(A); *Garrity*, 2002 WL 974676, at *3 (indicating that the Massachusetts Wiretap Act should be interpreted in accordance with the construction given to the Electronic Communications Privacy Act of 1986 (ECPA) by federal courts); Eagle Inv. Sys. Corp. v. Tamm, 146 F. Supp. 2d 105, 112 (D. Mass. 2001) (holding that the ECPA prohibits only acquisition of electronic communications that occur during transmission).

129. *Garrity*, 2002 WL 974676, at *3.

130. *Id.* at *4 (granting defendant's motion for summary judgment).

131. *See, e.g.*, *Garrity*, 2002 WL 974676, at *3–4; Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html.

132. *See, e.g.*, *Garrity*, 2002 WL 974676, at *3–4; *Bourke*, No. B068705.

133. *See, e.g.*, *Garrity*, 2002 WL 974676, at *3–4; *Bourke*, No. B068705.

1. Claims Invoking Antiquated State Statutes

Employee-plaintiffs relied on state statutes in an effort to carve out a respite of privacy protection in workplace technologies as far back as the early 1990s, when the technologies themselves were still in their infancy. *Bourke*, discussed at some length above, is illustrative.[134] Plaintiffs Bourke and Hall, disgruntled by Nissan's termination of their employment after the discovery of personal and sexual messages on their company e-mail, not only brought common-law and constitutional claims for invasion of privacy, but also asserted claims under two state statutes.[135] The first statute, California Penal Code section 631,[136] prohibited: "[I]ntentional[] tap[ping], or mak[ing] any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument, . . . or . . . read[ing], or attempt[ing] to read, or learn the contents of any message, report, or communication while the same is in transit or passing over any wire, line or cable . . . ."[137]

A separate provision afforded a civil remedy for the kind of wiretapping that the statute prohibits, but the court still rejected the claim because the statute did not cover "retrieval, printing and reading of E-mail messages."[138] Moreover, the court reasoned that the statute had no bearing on the case because Nissan, as the provider of the network service on which the subject e-mail messages were sent, received, and stored, did not need to "tap" into anything—the messages were readily available to Nissan on the system that it owned and operated.[139] Nor did Nissan access the messages during any transmission, as they were already in storage when Nissan reviewed them.[140] Thus, even while acknowledging the antiquated nature of the law, the court concluded summarily: "E-mail messages simply are not included within the actions proscribed by Penal Code section 631."[141]

The court adopted similar reasoning in rejecting the second statutory provision invoked by the *Bourke* plaintiffs, California

134. *Bourke*, No. B068705; *see supra* notes 28–43 (discussing *Bourke*).
135. *Bourke*, No. B068705.
136. CAL. PENAL CODE § 631 (West 2011).
137. *Bourke*, No. B068705 (quoting CAL. PENAL CODE § 631).
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*

Penal Code section 632.[142] That statute "prohibits the eavesdropping or recording of a 'confidential communication by means of any electronic amplifying or recording device.'"[143] The court found it inapposite just as readily as section 631: "Again, the plain words of the statute simpl[y] do not permit a finding that Nissan's conduct violated the law, as no amplifying or recording device was used to retrieve and read plaintiffs' E-mail messages."[144] The court rejected the plaintiffs' statutory claims wholesale, concluding that the statutes had no bearing on an employer's review of worker e-mail.[145]

The court in *Garrity*, considering a Massachusetts wiretap statute strikingly similar to the California provisions invoked in *Bourke*, reached the same result on nearly identical reasoning.[146] The subject statute, Massachusetts General Laws chapter 272, section 99, prohibits interception of wire and oral communications.[147] Just as did the court in *Bourke*, the *Garrity* court concluded swiftly that an employer's review of an employee's stored e-mail communications fell outside the ambit of the statute's protection: "Because the reading of e-mails, after they have been transmitted to the recipient, does not constitute 'interception' within the wiretap statute, plaintiffs' claim fails."[148] Further, the court also indicated that even if the kind of e-mail review conducted by the employer amounted to "interception" under the statute, it still might not apply because the statute's "ordinary business exemption" could protect the automatic back-up system on which the plaintiffs' reviewed e-mails were stored.[149] Thus, just as in *Bourke*, the court readily concluded that the state statute invoked by the plaintiffs applied only to more arcane forms of wire and oral communications and had no bearing on plaintiffs' gripes about Hancock's review of their e-mail.[150]

---

142. *See id.*
143. *Id.* (quoting CAL. PENAL CODE § 632).
144. *Id.*
145. *See id.*
146. *See* Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *3 (D. Mass. May 7, 2002).
147. *Id.*
148. *Id.*
149. *Id.*
150. *See id.*

2. Claims Premised on Evolving Federal Statutes

The original federal counterparts to the California and Massachusetts wiretap statutes at issue in *Bourke* and *Garrity*, respectively, likewise addressed only older forms of wire and oral communications and did not anticipate the changes that accompanied the evolution of electronic data and communication modes. As such, the original statutes were wholly ill-suited to redress the privacy claims of employees complaining that employers had improperly reviewed their electronic mail or other internet use in the workplace. Congress led the way in amending the subject statutes to account for the evolving technologies, but even so, the changes themselves are now antiquated and are not without their lingering shortcomings.

The decision of the United States Court of Appeals for the Fifth Circuit in *Steve Jackson Games, Inc. v. United States Secret Service* arose in a non-workplace setting but is nevertheless a precedent on which courts confronting workplace claims commonly rely for its interpretation of the federal statutes addressed to review and interception of wire and electronic communications.[151] The plaintiffs in *Steve Jackson Games* were the operator, Steve Jackson Games, Inc. (SJG), and users (various individuals) of an electronic bulletin board on which the users exchanged and stored e-mail messages related to SJG's business, which included role-playing games and related publications, among other things.[152] The United States Secret Service, in connection with an unrelated investigation, confiscated the SJG computer on which such e-mail messages were exchanged and stored.[153] Plaintiffs then sued, claiming that when the Secret Service

151. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission . . . . The first case to do so, *Steve Jackson Games*, noted that 'intercept' was defined as contemporaneous in the context of an aural communication under the old Wiretap Act . . . ."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876–77 (9th Cir. 2002) ("In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit held that the government's acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an 'interception' under the Wiretap Act . . . . We agree with the *Steve Jackson* [] court[] that the narrow definition of 'intercept' applies to electronic communications."); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

152. *Steve Jackson Games*, 36 F.3d at 458.

153. *Id.* at 459.

reviewed and deleted the "private" e-mail messages from the SJG computer, it violated the Privacy Protection Act,[154] the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA),[155] and Title II of the ECPA.[156]

Fruitful discussion of these statutes necessitates, as a precursor, some enlightenment on their historical development. The statutory scheme, which is at best described as "complex"[157] and perhaps more appropriately denominated as perplexing, includes the Federal Wiretap Act and both Titles I and II of the ECPA, the latter of which is commonly referred to as the Stored Communications Act (SCA).[158] The Federal Wiretap Act, out of which the other related laws have developed over time, originated as an effort to combat wiretapping and eavesdropping of the sort that permeated organized crime in the 1960s.[159] It was not until more than twenty years later that Congress added to the Wiretap Act protections for electronic communications as well, via the ECPA.[160] The ECPA, in turn, separated the protections it afforded electronic communications into two categories: (1) communications in transit, the "interception" of which was

---

154. Privacy Protection Act, 42 U.S.C. § 2000aa (2006). The Privacy Protection Act (PPA) makes it unlawful for the government, while conducting a criminal investigation, "to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication . . . ." *Id.* § 2000aa(a). The PPA is not directly relevant to this Article; as such, the plaintiffs' PPA claim in *Steve Jackson Games* does not warrant substantial attention or analysis here.

155. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012).

156. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

157. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("[T]he intersection of . . . [the Wiretap Act, as amended by the ECPA, and the SCA,] is a complex, often convoluted, area of the law." (internal quotation marks omitted)).

158. *See, e.g.*, 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 ("The privacy of stored Internet communications in the United States is governed by a federal statute known as the Stored Communications Act ('SCA'). The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act." (footnote omitted)).

159. *See generally* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 12–14 (2004) (discussing origin and enactment of Wiretap Act in 1960s).

160. 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.).

proscribed by Title I of the ECPA; and (2) communications in "storage," which were protected by Title II of the ECPA, also known as the SCA.[161] As explained by the Fifth Circuit:

> Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. In relevant part, § 2511(1)(a) proscribes "intentionally intercept[ing] . . . any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, *inter alia*, persons whose electronic communications are intercepted in violation of § 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. § 2520.[162]

Attempting to invoke the relatively new protections afforded by the ECPA, the *Steve Jackson Games* plaintiffs sued the Secret Service, claiming that its review of e-mail messages on the confiscated computer violated both Titles of the ECPA.[163] The district court awarded damages on the plaintiffs' Title II claim, finding that the Secret Service violated the SCA by seizing electronic communications (e-mail messages) stored on the confiscated computer.[164] Their claim under Title I, however, failed: "[The court] held that the Secret Service did not 'intercept' the E-mail in violation of Title I of the ECPA, 18

---

161. *Id.*; *see* Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2521 (2012); Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2012).

162. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (footnotes omitted). The Ninth Circuit has also offered a relatively pithy summary of the relevant statutory development:

> In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address the interception of . . . electronic communications." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act (SCA), which was designed to "address[ ] access to stored wire and electronic communications and transactional records."

Konop, 302 F.3d at 874.

163. *Steve Jackson Games*, 36 F.3d at 459. The plaintiffs also brought a claim under the federal Privacy Protection Act, but that claim, pertinent only to searches conducted in the course of governmental criminal investigations, is not relevant to this Article and thus is not discussed in any detail here.

164. *Id.*

U.S.C. § 2511(1)(a), because its acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications."[165] The sole question on appeal, then, addressed the propriety of the court's rejection of the Title I claim: "[W]hether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an 'intercept' proscribed by 18 U.S.C. § 2511(1)(a)."[166] The court engaged in a relatively lengthy analysis of the issue but ultimately upheld the district court's determination.[167] In a holding that paved the way for many other decisions that followed, the court concluded that the government's review of the e-mail messages on the confiscated computer did not violate the Federal Wiretap Act, as amended to include electronic communications, because that statute proscribes only "intercept[ion]" that is "contemporaneous with . . . transmission."[168] Notwithstanding that the plaintiffs had not yet retrieved some of the subject messages, no such interception occurred, because the messages were already in storage—the "transmission" of them, as contemplated by the Wiretap Act, had already transpired.[169]

The interpretation of the Wiretap Act and SCA offered by the court in *Steve Jackson Games* informed decisions of numerous courts that confronted similar statutory claims in the workplace setting in the years that followed. For example, in *Konop v. Hawaiian Airlines, Inc.*, the United States Court of Appeals for the Ninth Circuit relied on *Steve Jackson Games* for guidance and adopted similar reasoning in rejecting the plaintiff-employee's Wiretap Act/ECPA claim.[170] Plaintiff Konop, an airline pilot for defendant Hawaiian Airlines, created a website on which he posted criticisms of defendant, its officers, and the Air Line Pilots Association union.[171] Konop limited access to the website by requiring visitors to log in with a user name and password, and he provided login credentials

165. *Id.* at 459–60.
166. *Id.* at 460.
167. *See id.* at 460–63.
168. *Id.* at 460, 461–63.
169. *Id.*
170. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876–79 (9th Cir. 2002).
171. *Id.* at 872.

only to pilots and other employees of Hawaiian.[172] His plan to keep the site secret from management officials was foiled, though, when a vice president obtained login credentials from a willing employee and logged in multiple times to view Konop's content.[173] Upon learning of the vice president's access, Konop filed suit, alleging, among other things, violations of the federal Wiretap Act and the SCA.[174] The district court granted summary judgment to defendant, and Konop appealed.[175]

Addressing first the Wiretap Act claim, the Ninth Circuit on appeal readily concluded that Konop's website posts constituted "electronic communication" within the meaning of the statute, but nevertheless upheld the dismissal of that claim on grounds no unlawful "interception" occurred.[176] In reaching its conclusion, the court relied heavily on the interpretation of the Act offered in *Steve Jackson Games*.[177] Specifically, the *Konop* court found persuasive the Fifth Circuit's conclusion that the ECPA amendment retained stored communications within the definition of wire communications but omitted them from the definition of electronic communications.[178] As such, the statute elicited a narrow interpretation, by which electronic communications deserve protection only when in transit, and not while in storage.[179] Because Hawaiian viewed posts on Konop's website only when in storage, and not in transmission, his Wiretap Act claim failed.[180]

Konop's SCA claim, however, fared better. The district court had likewise granted summary judgment on the claim under the SCA, reasoning that although the SCA (not surprisingly) protects communications in storage and not just in transmission, the statutory exemption for access authorized by a "user" of the subject service applied, rendering Hawaiian's access lawful.[181] Because the employees who provided login credentials to the Hawaiian vice president were deemed "users," the district court reasoned that their involvement

172. *Id.*
173. *Id.* at 872–73.
174. *Id.* at 873.
175. *Id.*
176. *Id.* at 876–77, 879.
177. *Id.* at 876–77.
178. *Id.*
179. *Id.* at 877–78.
180. *Id.*
181. *Id.* at 879–80 (referring to the term of art "user" from 18 U.S.C. § 2701(c)(2) (2000)).

saved Hawaiian's conduct under the exemption, and Konop's SCA claim failed.[182] The Ninth Circuit, however, disagreed.[183] The statute defines a "user" as one who both *uses* the service *and* is duly authorized to do so.[184] But because the district court never made any findings as to whether the employees who provided their login credentials had ever actually *used* the website, the district court's ruling was flawed.[185] The Ninth Circuit therefore reversed entry of summary judgment on the SCA claim.[186]

The United States Court of Appeals for the Third Circuit, in *Fraser v. Nationwide Mutual Insurance Co.*, likewise adopted the reasoning of *Steve Jackson Games*, according a narrow interpretation to the ECPA so as to protect against only interceptions of electronic communications that occur in transmission.[187] Defendant Nationwide terminated plaintiff Fraser's employment as an insurance agent after searching his e-mail to ascertain the veracity of allegations that he was revealing company secrets to its competitors.[188] He subsequently sued in federal district court, alleging that Nationwide violated the ECPA when it searched his e-mail.[189] The court relied directly on *Steve Jackson Games* and *Konop* in affirming the rejection of Fraser's claim under Title I of the ECPA, adopting the same rationale to conclude that an employer's review of e-mail on its own server, even if without the sender/recipient-employee's permission, does not constitute unlawful interception within the meaning of the statute because the subject communications are no longer in transit, but rather are already in storage.[190] Furthermore, the court likewise rejected Fraser's claim under Title II of the ECPA (the

182. *Id.* at 880.

183. *Id.*

184. *Id.* (referring to 18 U.S.C. § 2701(c)(2)).

185. *See id.*

186. *Id.*

187. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003).

188. *Id.* at 110.

189. *Id.* He also brought claims for wrongful discharge, breach of contract, conversion, and invasion of privacy, but those claims are not relevant to this discussion of the federal statutory provisions. *Id.* at 110–11. The court affirmed dismissal of his conversion and invasion of privacy claims on procedural grounds, finding that the assertion of them by amendment was a mere dilatory tactic, *id.* at 116–17, and the court upheld rejection of his wrongful termination claim. *Id.* at 112–13.

190. *Id.* at 113–14.

SCA) on grounds that the "provider" exemption of the statute applied and protected the employer-provider's review of the employee's stored messages.[191] In very short order, the Third Circuit, following the trend well established by the pioneer courts that came before it, rejected wholesale the plaintiff-employee's attempt to invoke federal statutory protections, affirming in the process the employer's unfettered right to access any of the employee's electronic communications.[192]

C. EXTRACTING THE THEME

Although the facts and circumstances underlying each of these "early" technology-related workplace privacy cases differs, a persistent theme binds them together. In each and every one of these cases, the court took what might be described as an "easy way out," adhering to traditional notions of privacy and elementary conceptions of technologies that evolve faster than the wheels of justice can turn. In other words, shifting paradigms in workplace norms forged ahead in an effort to keep pace with the rapid changes in workplace technologies, but the courts' earliest decisions reflect a reluctance to keep pace.

The courts' decisions in the earliest of these workplace privacy cases lay a firm foundation for the theme for the others that followed. As the trailblazers, the California Court of Appeals in *Bourke v. Nissan Motor Corp.*[193] and the United States District Court for the Eastern District of Pennsylvania in *Smyth v. Pillsbury Co.*[194] both embody trepidation at confronting unfamiliar media and adhere to traditional notions of privacy and elementary conceptions of technology in adjudicating the employees' rights. In *Bourke*, the employees attempted to establish a reasonable expectation of privacy based on their right to restrict access to their work e-mail accounts via password-protection, but the court rejected those contentions without explanation, holding that regardless of their subjective understandings, their expectations of privacy

---

191. *Id.* at 114–15.

192. *Id.* at 113–15.

193. Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html; *see supra* notes 27–44 and accompanying text (discussing *Bourke*).

194. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); *see supra* notes 45–82 and accompanying text (discussing *Smyth*).

were not objectively reasonable.[195] Similarly, the court in *Smyth* rejected the plaintiff's privacy claims after his employer reviewed e-mail on his company account.[196] Even though the employer had assured him repeatedly that all e-mail communications were confidential and could not be used as grounds for termination or disciplinary action, the court nevertheless found, quite unequivocally, that any expectation of privacy he may have had in the e-mail messages was unreasonable and upheld his termination based on their content.[197] Indeed, the court in *Smyth* went so far as to declare boldly that, with respect to voluntary messages sent over a company e-mail system, "[w]e find no privacy interests in such communications."[198] In both of these earliest cases, then, the court not only gave short shrift to the plaintiffs' claims of privacy in e-mail communication, but it also did so in the face of employer assurances to the contrary and with little analysis to support its conclusions. Thus, these earliest privacy cases together suggest that the first courts to confront privacy claims in the context of workplace technologies had little interest in delving into either the evolving media or the potential for shifting social norms and instead disposed of the claims quickly and without regard to the employees' subjective expectations.

The next major case to come along, *McLaren v. Microsoft Corp.*, follows *Smyth* and, by distinguishing the traditional workplace privacy theories reflected in *K-Mart Corp. v. Trotti*,[199] shows remarkable reluctance to extend privacy rights recognized in those traditional (physical) settings to modern technologies.[200] Because the court in *McLaren* offers a bit more insight in the form of reasoning, its decision affords more fertile ground for critique than its precursors. The court's reasoning is, however, questionable. For example, the court distinguishes McLaren's e-mail from Trotti's locker on grounds the locker is discrete and separate, while an e-mail inbox is not.[201] Because

---

195. *Bourke*, No. B068705.

196. *Smyth*, 914 F. Supp. at 100–01.

197. *Id.* at 99–101.

198. *Id.* at 101.

199. K-Mart Corp. v. Trotti, 677 S.W.2d 632, 636–38 (Tex. App. 1984); *see supra* notes 101–12 and accompanying text (discussing *Trotti* and comparing that case with *McLaren*).

200. McLaren v. Microsoft Corp., No. 05–97–00824, 1999 WL 339015, at *4 (Tex. App. May 28, 1999); *see supra* notes 84–112 and accompanying text (discussing *McLaren*).

201. *McLaren*, 1999 WL 339015, at *4.

e-mail messages must cross the threshold of the employer's system before transfer to personal folders became possible, the court reasoned, those messages were not private by their very nature.[202] By contrast, the locker afforded Trotti a separate and distinct place to store her "tangible, personal belongings."[203] The court's distinction here reveals a fallacy of reasoning. In order for the contents of Trotti's locker to become in storage there, those personal belongings, not unlike McLaren's e-mail messages, would of necessity enter the employer's domain. The items stored in the locker did not appear there magically; Trotti placed them there only after carrying them into and through the threshold of the employer's building.

The *McLaren* court's approach also defies logic based on common lay understandings of how e-mail systems work. The court distinguished *Trotti* on the grounds that K-Mart provided the locker "for the specific purpose of storing *personal* belongings, not work items."[204] By contrast, the court reasoned, Microsoft provided McLaren's e-mail "so that he could perform the functions of his job."[205] As such, "the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment."[206] Again, the court's reasoning is flawed. It does not reflect the reality of electronic communications to assume that a worker will not make personal use of "personal folders" provided on the company's e-mail system, especially when the system invites the user to create a password to protect their contents.

One possible explanation for the flawed nature of the court's analysis in *McLaren* is that the court simply did not (indeed, perhaps even could not) understand the nature or the typical use of the technology at issue. While it certainly remains true that employers provide employees with e-mail accounts and networked computers from which to access them in order to enable performance of the employer's work, it is not consistent with reality to assume that, as a result, no personal use of the e-mail system occurs.[207] Whether the employer permits such use is a separate question, but the point remains

202. *Id*.
203. *Id*.
204. *Id*.
205. *Id*.
206. *Id*.
207. *See* Muhl, *supra* note 44, at 36.

true that the employee can (indeed, will) send and receive personal messages on a company-provided e-mail system.[208] Once that occurs, the employee is likely to store some or all of those messages in folders intended for that purpose. This is especially so where, as in *McLaren*, the e-mail system not only permits the establishment of "personal folders" but also enables the user to create his own password to protect them.

The courts that followed the trail blazed by *Bourke*, *Smyth*, and *McLaren* appeared quite content to stick to the same path, adhering to traditional notions of workplace privacy and refusing all invitations to extend any privacy protections to emerging technologies. The court in *Garrity v. John Hancock Mutual Life Insurance Co.* not only followed the lead of the precursor decisions, but it did so, at least with respect to the plaintiffs' common-law claims, by adopting wholesale their reasoning.[209] Indeed, the *Garrity* court offered very little in the way of its own original analysis, citing instead to *Smyth* and *McLaren*, and then leaping to the conclusion that the plaintiffs could not establish a reasonable expectation of privacy in their company e-mail accounts.[210] Like the precedents it followed, the *Garrity* court recognized that the employer had both expressly and impliedly, through its actions, indicated that it would not inspect employee e-mail (notwithstanding a reservation of rights to the contrary), but nevertheless refused to accord any common-law privacy rights to the employee plaintiffs.[211]

The *Garrity* court also refused to break any new ground in employee privacy under the statutes the plaintiffs had invoked. As to the statutory claims, it is difficult to say whether the refusal to recognize employee privacy in workplace electronic communications stemmed from a deep-seated reluctance to do so as a general matter, or instead was an inevitable conclusion in light of the underlying source laws—the antiquated statutes that had not kept pace with the evolving technologies. In that respect, *Garrity* and the other principal statutory cases from

208. *See id.*

209. Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002); *see supra* notes 113–30 and accompanying text (discussing *Garrity*).

210. *See Garrity*, 2002 WL 974676, at *1–2.

211. *Id.* at *2 ("Even if plaintiffs had a reasonable expectation of privacy in their work e-mail, defendant's legitimate business interest in protecting its employees from harassment in the workplace would likely trump plaintiffs' privacy interests.").

the "early" era,[212] *Konop v. Hawaiian Airlines, Inc.*,[213] and *Fraser v. Nationwide Mutual Insurance Co.*,[214] are all cut from the same cloth. Though *Garrity* addressed state statutes, while the claims in *Konop* and *Fraser* invoked federal law, the courts' treatment of those claims and interpretation of the similar statutes fall directly in line with one another.[215] In each of those cases, the court followed the lead of the United States Court of Appeals for the Fifth Circuit in *Steve Jackson Games v. U.S. Secret Service*,[216] interpreting the wiretap statute invoked by the plaintiff narrowly so as not to reach the employer's review of the employee's e-mail on grounds the messages in the employee's inbox (or e-mail folders, as the case may be), could not be "intercepted" within the meaning of the subject statute, because such messages were no longer "in transmission."[217]

Whatever reticence the courts in those early statutory cases might have felt when it came to charting new territory in employee workplace privacy, the statutes on which the plaintiffs were forced (absent any more readily applicable remedy) to rely likely obviated the results those courts reached, because the statutes themselves were highly antiquated and thus ill-equipped to address the needs of the rapidly evolving workplace. Indeed, in each of the subject cases, the plaintiffs attempted to carve out protections for communications made in a form that not only did not exist but indeed could not have been contemplated when the statutes themselves were enacted. Both the Massachusetts Wiretap Act invoked by the *Garrity* plaintiffs, and the Federal Wiretap Act relied upon by the plaintiffs in *Konop* and *Fraser*, had their origins in the war waged against organized crime in the 1960s.[218] As such, the

---

212. *See supra* Part I.A–B (identifying and discussing cases from the 1990s and early 2000s as comprising "early" workplace technology cases).

213. 302 F.3d 868 (9th Cir. 2002); *see supra* notes 170–86 and accompanying text (discussing *Konop*).

214. 352 F.3d 107 (3d Cir. 2003); *see supra* notes 187–92 and accompanying text (discussing *Fraser*).

215. *Compare Garrity*, 2002 WL 974676, at *3 (addressing the state wiretap statute), *with Konop*, 302 F.3d at 874–80 (addressing the federal wiretap statute), *and Fraser*, 352 F.3d at 113–15 (same).

216. 36 F.3d 457 (5th Cir. 1994); *see supra* notes 151–69 and accompanying text (discussing *Steve Jackson Games*).

217. *Fraser*, 352 F.3d at 113–14; *Konop*, 302 F.3d at 876–79; *Garrity*, 302 F.3d at *3.

218. S. REP. NO. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (discussing origins of the Wiretap Act as part of the Omnibus

statutes addressed only those forms of communication that existed at the time, focusing on the telephone.[219] Congress recognized these shortcomings and amended the federal statute in 1986 in an attempt to address modern technological advances, extending its protections to encompass "electronic" communications in addition to wire and oral ones, and covering not only such communications "in transmission" but also in storage.[220] In crafting the revised protections, Congress recognized the rapid evolution of the underlying technology, emphasizing the advent of communications via computer, computer networks, and private telephone lines.[221] But in the

---

Crime Control and Safe Streets Act of 1968); *Garrity*, 302 F.3d at *3 (indicating that the Massachusetts Wiretap Act is similar in purpose to its federal counterpart).

219. S. REP. NO. 99-541, at 2, *reprinted in* 1986 U.S.C.C.A.N. at 3556 ("[The Wiretap Act's] regimen for protecting the privacy of voice communications is expressly limited to the unauthorized aural interception of wire or oral communications. It only applies where the contents of a communication can be overheard and understood by the human ear. Furthermore, [it] applies only to interceptions of communications sent via common carriers." (citation omitted)).

220. *Konop*, 302 F.3d at 874 (discussing the 1986 amendment of the Wiretap Act to encompass interception and storage of electronic communications).

221. S. REP. NO. 99-541, at 2–3, *reprinted in* 1986 U.S.C.C.A.N. at 3555–57. The Senate Report described well the advancements and the concomitant need for statutory revision:

> Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing. A phone call can be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.
>
> These tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.
>
> Title I of the Electronic Communications Privacy Act addresses the interception of wire, oral and electronic communications. It

world of technology and electronic communications, what is "modern" one day is often antiquated the next. As such, the statutory revisions Congress made in 1986 were effectively outdated almost before they became effective, and certainly have not kept pace with the rapid and extensive changes that have occurred in the intervening quarter century.[222] Indeed, the statutes remain today in effectively the same form that they existed after the 1986 amendments.[223] As the *Konop* court explained well, the statutes are therefore wholly inadequate when it comes to redressing modern technological advancements:

> As we have previously observed, the intersection of [the Electronic Communications Privacy Act and the Stored Communications Act, both enacted as revisions to the Wiretap Act] is a complex, often convoluted, area of the law. In the present case, the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.[224]

Given these obvious inadequacies, it should come as no surprise that plaintiffs attempting to carve out protections in light of modern technologies have almost uniformly failed when attempting to rely on the antiquities of the statutory regime. As the *Konop* court forthrightly recognized—and then over a decade ago—the statutes will remain a wholly inadequate source of guidance when it comes to the rights and responsibilities of employees and employers in the modern workplace, at least until Congress succeeds in revising the laws to meet the rapidly evolving technologies.[225] While Congress

---

> amends existing chapter 119 of title 18 to bring it in line with technological developments and changes in the structure of the telecommunications industry.

Id.

222. *See Security and Surveillance*, CENTER FOR DEMOCRACY & TECH., https://www.cdt.org/issue/wiretap-ecpa (last visited Feb. 10, 2014) (discussing the impact of cloud storage and location tracking for mobile devices).

223. *See id.*

224. *Konop*, 302 F.3d at 874 (citations omitted) (internal quotation marks omitted).

225. *See id.*

has yet to confront the problem head on, though, new avenues may nevertheless be emerging.

II. RECENT DEVELOPMENTS IN WORKER PRIVACY

Change is afoot. In the latter part of the new millennium's first decade, the law of worker privacy began what appears to be a modern evolution, pacing behind but nevertheless reflective of shifting social norms as technology growth burgeoned, and its use in and beyond the workplace became pervasive. The evolution is far from complete, and remains in a state of vulnerable infancy. Its trajectory is likely to change many times in the decades to come. Yet, the trends reflected in the law are unmistakable, and suggest that as the use of technology becomes increasingly widespread, the law may follow in recognizing the need for some privacy protections that did not previously exist.[226]

This Part discusses recent developments in the law concerning employee privacy in workplace technologies, and suggests that the trend appears to be favoring broader recognition of employee privacy in at least those uses of technology that are becoming the most widely accepted. Venturing into uncharted territory, a few progressive courts led the way by acknowledging for the first time that employees may reasonably expect privacy in workplace technologies.[227] Following that trend, some courts have found new paths around antiquated statutes to carve out new rights, while state legislatures have begun enacting new laws to protect their constituents in the modernizing world.[228] These common-law and statutory trends are also bleeding over into the realm of administrative law, as agencies have followed suit by recognizing that employees may retain privacy rights to protect their online social networking, even when it directly impacts the workplace.[229] This section discusses each of these

---

226. *See infra* Part II.A.1.

227. *See infra* Part II.A.1.

228. *See, e.g.*, *Employer Access to Social Media Usernames and Passwords*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last updated Mar. 21, 2014) (discussing pending state legislation to prevent employers from requiring access to personal social media accounts).

229. *See, e.g.*, Steven Greenhouse, *Company Accused of Firing Over Facebook Post*, N.Y. TIMES, Nov. 8, 2010, http://www.nytimes.com/2010/11/09/business/09facebook.html?_r=0 (discussing a complaint brought by the

developments in turn and reveals in the process a distinct trend away from the reluctance and trepidation of the prior generation, in favor of broader privacy rights for the high-tech workforce.

A. THE COMMON-LAW TRAILBLAZERS

The evolution of workplace privacy rights in emerging technologies began when a few trailblazing judges became the first to recognize that employees may reasonably expect privacy in e-mail sent over or accessed on company equipment. Remarkably, some of these judges recognized such privacy expectations even in the face of published company policies attempting to defeat those very expectancies. As the first, or at least foremost, courts to balk the firmly entrenched disdain for worker privacy in emerging technologies that permeated the law of the late 1990s and early twenty-first century, their decisions paved the path for further evolution that has indubitably begun but has yet to reach fruition. The cases discussed below, while not the only ones that might fall into this category, typify and exemplify the shifting norms of the modern era.

1. State and Federal Court Decisions According Broader Common-Law Privacy Rights

The United States District Court for the Southern District of New York led the way into the modern era of workplace privacy by condoning employee privacy claims in e-mail messages accessed on company equipment, notwithstanding the employer's policy attempting to defeat any expectation of privacy.[230] Notably, the context for that court's 2008 decision in *Pure Power Boot Camp v. Warrior Fitness Boot Camp* departed from the traditional model by which the earlier privacy cases came to the attention of the courts. The privacy issue in *Pure Power Boot Camp* arose not as the central tenet of the plaintiffs' claims, as it had in the wrongful discharge and invasion of privacy cases of the "early" era,[231] but instead as a

---

National Labor Relations Board on behalf of an employee fired after complaining about her boss on her Facebook account).

230. *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561–62 (S.D.N.Y. 2008).

231. *See supra* Part I.A.1 (discussing early cases involving claims to worker privacy in new technologies, such as *Bourke v. Nissan Motor Corp.* (rejecting claims for common-law and constitutional invasion of privacy), and *Smyth v.*

peripheral matter raised via an evidentiary objection.[232] Indeed, the central claims in that case did not involve worker privacy at all. Instead, the plaintiff Pure Power Boot Camp (PPBC), which formerly employed the individual defendants, sued them and the competing fitness center (defendant Warrior Fitness Boot Camp) they had recently opened, bringing various claims for breach of restrictive covenants, breach of fiduciary duties, and infringement of trademarks, trade dress, and copyrights.[233] The plaintiffs attempted to rely in the course of the litigation on thirty-four e-mail messages obtained by PPBC representatives from an individual defendant's e-mail accounts, but the defendants objected on privacy grounds.[234]

The context in which the privacy issue arose in *Pure Power Boot Camp* made it a good candidate to begin shifting the tide away from reluctance and toward acceptance of employee privacy in e-mail. First, as explained above, the issue arose as a peripheral evidentiary matter and not as the foundation of the plaintiffs' claims. As such, at least arguably, the court could approach the privacy law aspect somewhat more aggressively, without having to depart blatantly from established precedents or disregard principles of *stare decisis*. Moreover, the factual context made it a persuasive case for recognition of employee privacy rights because, unlike in many of the "early era" cases,[235] it was not clear that the subject employee e-mails had been created on employer equipment or during the employee's working hours.[236] PPBC gained access to the subject e-mail messages, which were sent from the defendant's personal web-based e-mail accounts (Gmail.com, Hotmail.com, and warriorfitnessbootcamp.com, an account on his new employer's domain), after he left his Hotmail username and password stored on PPBC's computers.[237] Because he used the same

---

Pillsbury Co. (dismissing a privacy-based claim for wrongful discharge in violation of public policy)).

232. *Pure Power Boot Camp*, 587 F. Supp. 2d at 551.

233. *Id.*

234. *See id.* at 551–52.

235. *See supra* Part I.A (discussing early cases raising issues pertaining to employee privacy in workplace technologies).

236. *See Pure Power Boot Camp*, 587 F. Supp. 2d at 553 n.3 ("[Defendant] Fell makes a general claim that he never did any work related to WFBC while he was at PPBC or on PPBC computers. However, he has not provided his PPBC work schedule, so there is no way to confirm whether or not he was at PPBC when he sent any of these e-mails." (citation omitted)).

237. *Id.* at 552.

password for his other e-mail accounts, PPBC was able to access those accounts as well.[238] Thus, the employee had used his employer's computer to access his personal e-mail at one time, but there was otherwise no proof that he used company equipment to create the subject messages on a later date, or that he did so while he was working.[239] Chiefly relying on these facts, the court concluded that the defendant reasonably expected privacy in the e-mail messages he sent, received, and stored on his personal accounts, even though he had not only accessed those accounts on employer equipment but had also saved his password there, enabling one-click account entry by anyone who could turn on the computer.[240] What is more, the court recognized these privacy rights, in the face of an employer policy that expressly negated any privacy rights or expectations in any e-mail that passed through the company's computer system.[241]

The reduced connection in *Pure Power Boot Camp* between the e-mail messages in which the (here, former) employee claimed privacy, on the one hand, and the employer's workplace, on the other, opened the door for the court to confer greater privacy-based protection than had been recognized in the technology-based privacy cases that preceded it.[242] And yet, the principles that the court announced and the analytical approach it took leave room for courts to follow its lead in subsequent cases, expanding the privacy rights that the *Pure Power Boot Camp* court initially pronounced. Of chief importance in that regard is the fact that the court recognized privacy rights in the face of an employer policy attempting to

---

238. *Id.*

239. *Id.* at 553.

240. *Id.* at 560–61.

241. *See id.* at 552–53. Specifically, the PPBC Employee Handbook policy concerning e-mail access on company computers stated:

> [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*. *The Company*, in its discretion *as owner of the E-Mail system*, reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through *the system*, for any reason, without the permission of any system user, and without notice.

Id.

242. *See id.* at 560–61.

defeat any such expectation or claim.[243] In reaching that conclusion, the court distinguished the facts of the case before it from those in which courts had relied directly on similar policies to reject employee privacy claims, on grounds the PPBC employee had not actually stored any of the subject e-mail messages on company equipment and likely had not even sent the messages from, or received them on, employer equipment.[244] Yet, the employee had not only *accessed* his personal account on PPBC's computer, but he had also gone so far as to store his password there as well, leaving the door wide open to any person who powered it on.[245] The court dismissed these facts as essentially irrelevant, though, holding that saving the password did not confer implied consent to access the account's contents, and that his privacy expectation in the personal account therefore remained intact.[246] As such, the *Pure Power Boot Camp* decision charts new territory, by comparison to the "early era" cases discussed above, in that it upholds an employee's right to privacy in the face of a policy attempting to directly defeat the same, and when the employee had himself essentially provided the employer the "key" to his account by saving his password on company equipment.[247] Moreover, the decision also sets a strong precedent concerning the strength of privacy claims in the context of technologies established personally by the employee (here, personal web-based e-mail accounts), even when the employee accesses those technologies on the employer's equipment or network, and even where the employee provides sufficient information to allow the employer ready access.

Subsequent courts addressing employee privacy claims in similar yet distinct contexts seemed to follow the lead of the *Pure Power Boot Camp* court in expanding common law protections of employees' technology-based privacy rights, even if they did not rely on that case expressly. For example, in *Pietrylo v. Hillstone Restaurant Group*, the court held that the plaintiff-employees had proffered sufficient evidence to reach a jury on their claims that the employer invaded reasonably

---

243. *See id.* at 552–53, 559–62.

244. *Id.* at 560.

245. *Id.* at 552.

246. *Id.* at 561.

247. *See id.* (employing a house-key analogy in explaining that storing a password on a computer is equivalent to leaving a key on a doorstep, which does not confer consent to entry).

expected privacy when it accessed a website created by and for the employees for the purpose of "vent[ing] about . . . work without any outside eyes spying in on us."[248] The plaintiffs, former employees of the defendant company that operated a Houston's restaurant where they had worked, were discharged after management discovered postings on an employee-run Myspace.com page that management found "offensive" as well as contradictory to the restaurant's core values of "professionalism, positive mental attitude, aim to please approach, and teamwork."[249] The plaintiffs had set up the page as a forum in which employees could share frustrations about their jobs.[250] Management gained access to the page when one of the member-employees shared her password with them.[251]

After the company terminated their employment due to the offensive content found on the Myspace.com page, the plaintiffs sued, bringing both statutory and common law claims.[252] Unlike the predecessor plaintiffs of the earlier era, the Houston's plaintiffs received a warmer reception to their privacy pleas. Indeed, not only did the plaintiffs' privacy claims survive an early motion to dismiss[253]—the stage at which several of the early-era claims faltered[254]—but they even triumphed over a motion for summary judgment, with the next stop the proverbial plaintiffs' promised land of a trial by jury.[255] Specifically, four of plaintiffs' claims, all with privacy implications, survived defendant's summary judgment motion: statutory claims under the federal Stored Communications Act and its state-law counterpart, a tort claim for wrongful termination in violation of public policy premised on an alleged

---

248. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008). The claims that survived defendant's motion for summary judgment consisted of alleged violations of the Stored Communications Act and a state counterpart statute, a claim for wrongful discharge in violation of public policy based on an invasion of privacy, and a common-law claim for the tort of invasion of privacy itself. *See id.* at *3–7.

249. *Id.* at *2.

250. *See id.* at *1.

251. *Id.*

252. *Id.* at *2.

253. *Id.*

254. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996) (dismissing plaintiff's privacy claims after employer terminated plaintiff employee for content of e-mail messages); *see also supra* notes 45–82 and accompanying text (discussing *Smyth* and its resolution on a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6)).

255. *See Pietrylo*, 2008 WL 6085437, at *3–7.

invasion of privacy, and a tort claim for invasion of privacy standing alone.[256]

As to the statutory claims, the court focused on the fact that the employee who granted access to management by sharing her password did so only out of concern for her job, fearing that adverse employment action may be taken if she did not comply.[257] In light of her testimony that she felt pressured into sharing her password in order to protect her job, the court concluded that a genuine issue of fact existed concerning whether her consent was voluntary.[258] Suggesting that consent offered only under duress would not constitute the requisite authorization to afford a liability exemption under the statutes, the court denied the defendant's motion for summary judgment.[259] Thus, the court readily found an avenue by which it could permit the plaintiffs' claims to proceed.

The plaintiffs' common-law claims met with similar success, affording an even starker contrast to the fate of comparable claims brought in the early era. First, quite unlike the first courts to confront the issue, the *Pietrylo* court readily concluded that "[a] right to privacy may be a source of 'a clear mandate of public policy' that could support a claim for wrongful termination."[260] Moreover, the court did not hesitate in finding that the plaintiffs reasonably expected privacy in their "invitation-only internet discussion space,"[261] notwithstanding that the employees used the company logo to label the page and gathered together there only because of their workplace connection.[262] Again relying on facts concerning the conditions under which the managers gained access to the site, the court concluded that a disputed issue of material fact regarding authorization necessitated resolution by trial.[263] Similarly, the authorization issue precluded summary judgment on the plaintiffs' common-law invasion of privacy claim, as well.[264] And unlike the predecessor courts of the earlier era, the *Pietrylo* court readily concluded that the

256. *See id.* at *3–7.
257. *See id.* at *4.
258. *Id.*
259. *Id.*
260. *Id.* at *6.
261. *See id.*
262. *See id.* at *1.
263. *See id.* at *6.
264. *Id.* at *7.

employees might have reasonably expected privacy in their postings, even though the site existed on the World Wide Web, because of the fact that the employees protected it with a password.[265] In that respect, the *Pietrylo* case stands in stark contrast to the cases of the early era, in which courts tended to swiftly reject employee privacy claims even as to messages sent on individual employees' e-mail accounts, which are at least arguably more prone to expectations of privacy than postings to a web site.[266] What was wholly inadequate to survive an out-of-the-gates motion to dismiss in the early era, became readily sufficient to support the claim's viability not only at the initial stages but even all the way to trial.

The trajectory toward increasingly open reception to employee privacy claims stemming from technology use reached new heights in the 2010 New Jersey Supreme Court case, *Stengart v. Loving Care Agency, Inc.*[267] Perhaps most notably, and consistent with the approach of other modern-era courts, the *Stengart* court gave short shrift to the employer's policy unequivocally negating any expectation of privacy in actions taken on company computer equipment.[268] Instead, the court dismissed the published policy as irrelevant because the employee sent and received the subject e-mail messages via her own personal, password-protected, web-based e-mail account, even though she did so on the company's equipment, as expressly contemplated by the policy.[269] Indeed, although the context of the privacy issue in *Stengart* bore striking similarities to that presented in the case decided just two years earlier by the neighboring New York federal district court in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*,[270] the

---

265. *See id.* Indeed, the court held that a genuine issue of material fact existed concerning whether the employees reasonably expected privacy in their web postings. *Id.*

266. *See id.*; *see also supra* Part I.A.1 (discussing courts' swift rejection of employee privacy claims stemming from employers' review of employee e-mail messages).

267. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

268. *See id.* at 657–58; *see also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 559–60 (S.D.N.Y. 2008) (rejecting employer's claim that policy purporting to negate expectation of privacy was effective as to e-mail messages sent on employee's personal, password-protected, web-based e-mail account).

269. *See Stengart*, 990 A.2d at 657.

270. *See Pure Power Boot Camp*, 587 F. Supp. 2d at 552–53; *supra* notes 230–47 and accompanying text (discussing *Pure Power Boot Camp*).

Stengart court arguably extended its recognition of privacy rights even further.

As in *Pure Power Boot Camp*, the privacy issue in *Stengart* did not form the foundation of the plaintiff's lawsuit, but instead arose out of a discovery dispute.[271] The plaintiff, Marina Stengart, sued her former employer, defendant Loving-Care Agency, alleging constructive discharge, harassment, and retaliation.[272] After she filed suit, Loving Care hired a computer forensic expert to mine data off the company laptop she had used during her employment, and found a number of e-mail messages exchanged between Stengart and her attorney via her personal, password-protected, web-based e-mail account.[273] When Loving Care relied on those e-mail messages during discovery, Stengart objected, asserting the attorney-client privilege and seeking return of the e-mails.[274]

The trial court's decision tracked more closely the sentiments of the earlier era, triumphing employer prerogative over employee rights, but the appellate courts found otherwise.[275] The company's Electronic Communication Policy, which carried the day at the trial court, purported to negate any expectation of privacy in any use to which an employee might put her company-issued equipment:

> The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice . . . . E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.[276]

According to the trial court, because the policy expressly stated that Internet communications on company equipment were "not to be considered private or personal," plaintiff Stengart could not claim any protection—via the attorney-client privilege or otherwise—of her e-mails sent on her laptop.[277] The court of appeals, and eventually the New Jersey Supreme Court, however, disagreed.[278] Reading the employer's policy

---

271. *See Stengart*, 990 A.2d at 655.
272. *Id.*
273. *Id.*
274. *Id.*
275. *Id.*
276. *Id.* at 657.
277. *Id.*
278. *See id.* at 655.

narrowly in favor of employee rights, the appellate courts held instead that Stengart retained an expectation of privacy in her webmail communications, based primarily on its conclusion that the employer's policy did not address "personal [e-mail] accounts."[279] Because she did not expect that the company could and would access the personal webmail she sent on her company laptop, she did not waive the attorney-client privilege when she used that equipment to send the subject messages.[280] As such, the *Stengart* court, consistent with other modern-era decisions, stepped out from the bonds of employer prerogative that led to broad application of electronic communication policies in the early era, and readily concluded instead that because the subject policy did not expressly describe the employer's ability to access *any* Internet usage on its own equipment, the policy simply did not govern.[281]

2. Supreme Court Instruction—Or the Lack Thereof

Taken together, the cases discussed above—*Pure Power Boot Camp*,[282] *Pietrylo*,[283] and *Stengart*[284]—though far from the *only* decisions on the subject in recent years, represent well the modern consensus and its trend away from the trepidation reflected in decisions rendered in the earlier years of the modern technological era. In each of those three representative cases, the court employed traditional common law doctrine concerning employees' expectations of privacy, but departed

279. *See id*. at 657.

280. *See id.* at 663–65.

281. *See id.* The *Stengart* court also discussed other similar decisions that might fairly be grouped along with it as representative of the trend toward increasing recognition of employee privacy rights in the modern era. *See, e.g.*, *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 259 (Bankr. S.D.N.Y. 2005) (finding that because employer policy purporting to ban personal use of e-mail and allowing monitoring was "equivocal," employee could claim attorney-client privilege in e-mail messages exchanged with lawyer over company e-mail system); Memorandum and Order on Plaintiffs' Motion to Compel at *3, Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006) (No. 04-2618-BLS2) (finding that employee had reasonable expectation of privacy in webmail messages sent on company computer because employer's Internet communications policy "did not expressly declare that it would monitor the *content* of Internet communications").

282. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008); *see supra* notes 230–47 and accompanying text.

283. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008); *see supra* notes 248–66 and accompanying text.

284. *Stengart*, 990 A.2d 650; *see supra* notes 267–81 and accompanying text.

from the reluctant ways of the predecessor courts by narrowly interpreting employer monitoring policies or otherwise finding that employee privacy rights prevailed notwithstanding employers' attempts to defeat them.[285] These representative cases paint a thorough picture of the shifting norms that underlie the modern era, but a discussion of cases addressing the courts' approach to common-law notions of privacy expectations would not be complete without at least mentioning the United States Supreme Court's dabbling in this arena. And while the High Court's decisions that address reasonable expectations of privacy in the workplace typically arise in the context of constitutional questions relevant only in the public workplace—a body of law that lies only at the periphery of this Article—its instruction is nevertheless pertinent, as other courts interpreting the common law often look to the Supreme Court's jurisprudence in the constitutional setting for guidance.[286]

The Supreme Court's body of law assessing employee privacy in the public workplace setting is relatively rich both in history and in depth, but it is the Court's 2010 decision in *City of Ontario v. Quon* that is most relevant here.[287] The Court's decision in *Quon*—or, perhaps more accurately, its refusal to reach any decision about privacy expectations—failed to provide the instruction that many hoped it would afford, but is nevertheless not entirely useless. Indeed, the Court's discussion of privacy expectations might best be characterized as paving the way for courts to follow the lead of those discussed above in taking a more aggressive, and progressive, approach to issues of employee workplace privacy in the technological era.

Quon is especially pertinent here because it was the first Supreme Court case to address employee privacy rights in workplace technologies. Jeff Quon, a police officer and SWAT Team member in the city of Ontario, California, sued the City alleging constitutional violations after City officials reviewed

---

285. *See, e.g.*, *Pure Power Boot Camp*, 587 F. Supp. 2d at 561.

286. *See, e.g.*, Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 897–99 (Cal. Ct. App. 2011) (discussing, at length, case law on workplace privacy rights, dismissing that body of law as not directly relevant to the private setting, but proceeding to apply principles announced in those cases to assess plaintiff's privacy claims).

287. *See* City of Ontario v. Quon, 560 U.S. 746 (2010).

text messages sent and received on his City-issued pager.[288] Prior to issuing the employee pagers, the City announced a "Computer Usage, Internet, and E-mail Policy," reserving the City's right to monitor "all network activity" and specifying that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[289] Although the policy did not apply on its face to text messages, the City announced on several occasions that it would accord the same treatment to text messages as it did to e-mail and other network usages.[290] In addition, a supervisor expressly told Quon "that messages sent on the pagers were 'considered e-mail and could be audited,'" though that same supervisor also went on to explain that "it was not his intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions."[291] When Quon regularly exceeded the monthly character limitation on his text messaging plan, his superiors in the police department attempted to ascertain whether the overages warranted an increase in his character allotment.[292] In order to make that determination, the department obtained text-message transcripts from Arch Wireless, the third-party service provider, and reviewed them for content.[293] In an apparent effort to preserve Quon's privacy, the officer consulted Quon's work schedule and redacted any messages sent during non-working hours, but nevertheless found that the majority of messages sent and received on Quon's pager, even during work hours, did not pertain to his job.[294] The City disciplined Quon as a result of these findings.[295]

Of central significance here is the Court's discussion of Quon's privacy expectations in this setting, which arose as an

---

288. *See id.* at 750–53.
289. *Id.* at 751.
290. *See id.* at 751–52.
291. *Id.* at 752.
292. *See id.* at 752.
293. *Id.*
294. *Id.* at 753. The officer's report noted that:

> Quon sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business.

Id.
295. *Id.*

issue as part of his claim under 42 U.S.C. § 1983 that the City violated his constitutional protections against unlawful searches under the Fourth Amendment.[296] The Court's precedents addressing employee privacy in the public workplace had not yielded a consensus rule concerning either the requisite proof to make out a claim, or the parameters of reasonable privacy expectations pertinent thereto.[297] Instead, the Court's only precedents had failed to garner support of a sufficient majority of justices to elicit a majority rule.[298] In particular, the 1987 decision in *O'Connor v. Ortega*, although the seminal authority on the privacy rights of public employees under the Fourth Amendment, emerged as only a plurality opinion.[299] A four-justice plurality, led by Justice Sandra Day O'Connor, favored a two-step process for the assessment of public employees' Fourth Amendment rights.[300] According to the plurality, a court must first consider "'[t]he operational realities of the workplace' in order to determine whether an employee's Fourth Amendment rights are implicated. On this view, 'the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.'"[301] If such an expectation can reasonably be found, then, according to the plurality, a court should proceed to determine whether an employer's intrusion on that expectation is reasonable under the circumstances.[302] This two-part test did not, however, become the definitive rule, because it failed to garner support from a majority of justices. The other view, espoused and articulated by Justice Antonin Scalia, "would have dispensed with an inquiry into 'operational realities' and would conclude 'that offices of government employees . . . are covered by Fourth Amendment protections as a general

---

296. *Id.* Quon also brought claims under the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006), as well as California state law, but those claims were not before the Supreme Court in this case and otherwise lie beyond the scope of this Article due to the public employment setting in which the case arose and the existence of third-party service provider Arch Wireless as a defendant in the case as originally filed. *Id.* at 753.

297. *See id.* at 757 (explaining lack of clarity concerning a "threshold test for determining the scope of an employee's Fourth Amendment rights").

298. *Id.*

299. *Id.* at 756–57 (discussing O'Connor v. Ortega, 480 U.S. 709 (1987)).

300. *Id.* at 756.

301. *Id.* at 756–57 (quoting *O'Connor*, 480 U.S. at 717–18) (citation omitted).

302. *Id.* at 757 (discussing *O'Connor*, 480 U.S. at 725–26).

matter."[303] Justice Scalia would then have proceeded directly to an assessment of the reasonableness of the search itself, with the instruction "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment."[304] Thus, while the plurality would have conducted a threshold inquiry into whether the employee reasonably expected privacy, Justice Scalia would assume that expectation and consider only whether the search was reasonable, tapping into private-workplace norms in making that assessment.

In the nearly quarter century that passed between *O'Connor* and the Court's grant of certiorari in *Quon*, the lower courts floundered in the absence of a majority rule concerning the governing framework.[305] Many adopted the plurality approach, thereby necessitating inquiry into the employee's privacy expectations.[306] Whether the "right" approach or not, the plurality's two-part test has the advantage of fostering development of the law concerning the reasonableness of employee privacy expectations which, although not directly binding in common-law cases, is nevertheless instructive. Thus, many hoped that when the Supreme Court granted review of the Ninth Circuit's decision in *Quon*, it would not only answer the proof-structure question left open after *Ortega*, but would also provide some of that very sort of instruction concerning employee privacy in the age of technology.[307]

---

303. *Id.* (quoting *O'Connor*, 480 U.S. at 731 (Scalia, J., concurring)).

304. *Id.* (quoting *O'Connor*, 480 U.S. at 732 (Scalia, J., concurring)).

305. *See, e.g.*, Shields v. Burge, 874 F.2d 1201, 1203–04 (7th Cir. 1989) (attempting to discern governing rule of law from *O'Connor* in light of plurality opinion); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1333–34 (9th Cir. 1987) (discussing splintered opinions in *O'Connor*).

306. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (stating that Justice O'Connor's approach from the *O'Connor* plurality opinion controls); *Shields*, 874 F.2d at 1203 (same); *Schowengerdt*, 823 F.2d at 1334 (same).

307. *See* David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 622 (2010) (discussing expectantly that the Supreme Court had granted certiorari to review Ninth Circuit's decision in *Quon* and stating that "[t]his is an opportunity for the Court to speak directly on the privacy protections available for electronic communications delivered through third parties"); Clifford S. Fishman, *Electronic Privacy in the Government Workplace and* City of Ontario*,* California v. Quon*: The Supreme Court Brought Forth a Mouse*, 81 MISS. L.J. 1359, 1362–63 (2012) ("When the Court granted cert in

Unfortunately, the speculators were disappointed. Although the case did produce a majority opinion, it did not resolve the open question concerning the proof framework applicable to public employee Fourth Amendment cases.[308] Instead, the Court dodged that question by concluding that the search was reasonable, thereby obviating the need for inquiry into whether Quon had a reasonable expectation of privacy or not.[309] As such, "[t]he two *O'Connor* approaches—the plurality's and Justice Scalia's—therefore lead to the same result."[310] No answer emerged, and the lingering proof-framework question remains open.

The Court's failure to resolve the open proof-framework question is disappointing, but what is even more troublesome, at least for purposes of this Article, is the absence of any useful guidance in the opinion about reasonable expectations of privacy in workplace technologies. There was no need to address that issue at all, given the majority's conclusion that the search was reasonable regardless of Quon's expectations.[311] Nevertheless, in the spirit of "instruct[ion]," the majority went on to discuss whether Quon had a reasonable expectation of privacy in the text messages on his pager.[312] However, its "instruction" fell far short of deserving that label. The most instructive point that can be gleaned from the Court's dictum is that in assessing privacy expectations, workplace policies and practices matter.[313] That point, however, is far from novel. Indeed, nearly every one of the cases discussed above addressed the employer's policy concerning technology use as relevant to the employee's privacy expectations, at least in some respect.[314] Beyond that point, the Court expressly refused to delve any further, reciting the rapid evolution of technology

---

Quon . . . many scholars, judges, and practitioners hoped that the *Quon* decision would clarify the uncertainties left over from *O'Connor* and resolve new issues created by electronic communications technology. On the other hand, some observers feared that the Court in *Quon* might issue a broad, sweeping decision that could have a substantial, unforeseeable, and perhaps unfortunate impact on emerging communications technologies. As it turned out, *Quon* decided very little, and leaves the law more unsettled than it previously was.").

308. *Quon*, 560 U.S. at 757.
309. *Id.*
310. *Id.*
311. *Id.*
312. *Id.* at 758–59.
313. *Id.* at 758.
314. *See, e.g.*, *supra* Parts I.A.1, II.A.1.

as good reason to avoid broaching the topic of a legal response to it.[315] Indeed, the Court went on at some length here, taking pains to make clear its trepidation about resolving questions concerning privacy expectations in the face of rapidly shifting social norms:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear . . . .
>
> . . . .
>
> . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[316]

Thus, the Court *stated* that it was loathe to dictate the parameters of proper inquiry into privacy expectations in workplace technologies, but it nevertheless proceeded to do much of what it disclaimed. The Court identified a variety of relevant factors, including the employer's policies and communications to employees, the pervasiveness of the subject technologies, and society's expectations about them at large, but it did so without supplying any real parameters to guide the inquiry.[317] The result is therefore subjectivity and lack of predictability.

The Court's refusal to address privacy expectations on grounds that it must proceed cautiously due to the rapid evolution of the relevant technologies is somewhat ironic given that the very technologies at stake—text messages sent via paging devices—were heavily antiquated by the time the Court rendered its decision. Justice Scalia, concurring in the judgment, boldly chastised the majority for its timidity:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we

315. *Quon*, 560 U.S. at 759–60.
316. *Id.*
317. *Id.*

> have no choice. The Court's implication . . . that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for the disregard of duty.[318]

According to Justice Scalia, then, the majority went too far in "instructing" about privacy expectations at all.[319] Moreover, the instruction itself elicited his negative response on grounds that it will cause lower courts to flounder in their analysis of privacy issues and reach erroneous results more often than not.[320] As is often the case, Justice Scalia's point is best made by extracting his very words:

> Worse still, the digression is self-defeating. Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described "instructive" expatiation on how the *O'Connor* plurality's approach would apply here (if it applied) as a heavy-handed hint about how *they* should proceed. Litigants will do likewise, using the threshold question whether the Fourth Amendment is even implicated as a basis for bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of electronic media. In short, in saying why it is not saying more, the Court says much more than it should.[321]

Given the ambiguity in the non-exhaustive list of relevant considerations that the majority offered in its dictum, Justice Scalia's criticisms have some resonance. As discussed in Part III below, his suggestion that any standard necessitating a subjective inquiry into the norms surrounding rapidly evolving technologies makes some sense, and may imply a route out of the maze of complicated legal questions in this area of the law.

B. REINTERPRETATION OF OLD STATUTES AND ENACTMENT OF NEW ONES

The modern era in the law of employee privacy ushered in more expansive interpretations of common-law notions of privacy, as the cases discussed in the preceding section illustrate. Expansion of rights under the common law is not the only path by which the law in this area is evolving, though.

---

318. *Id.* at 768 (Scalia, J., concurring).
319. *Id.* at 768–69.
320. *Id.*
321. *Id.* (citation omitted).

Statutes applicable to workplace technologies are also supplying greater privacy protection. While courts afford broader or otherwise more protective interpretations to the antiquated statutes that have been on the books for some period of time, legislative bodies at both the state and federal level are also responding to the evolution of workplace technologies and social norms. This section addresses both avenues of expansion, discussing representative cases according more protective interpretations to pre-existing statutes as well as statutory reform efforts.

1. Modernized Interpretation of Antiquated Statutes

It is beyond objection that the existing statutory framework relevant to employee privacy in workplace technologies is highly antiquated and ill-suited to answer the legal questions that arise in the modern era.[322] Indeed, the only relevant federal statutes, enacted in 1986, are approaching thirty years old and pre-date the advent of the Internet and World Wide Web.[323] Those statutes, the Electronic Communications Privacy Act (ECPA)[324] and Stored Communications Act (SCA),[325] originally afforded little to no protection for employees seeking a privacy refuge, as discussed in much more detail in Part I of this Article.[326] That is, the ECPA was interpreted to protect only against interception of communications contemporaneous with transmission.[327] As such, it typically had no application with respect to e-mail communications, which are nearly always accessed only after delivery to the intended recipient's account.[328] The SCA, as its name connotes, does afford protection to electronic communications after they are in storage.[329] However, the

322. *See*, *e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (stating that the "existing statutory framework is ill-suited to address modern forms of communication").

323. *Id.*

324. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012); *see supra* Part I.B.2 (discussing origin of ECPA and SCA).

325. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); *see supra* Part I.B.2 (discussing origin of ECPA and SCA).

326. *See supra* Part I.B.2 (discussing cases interpreting ECPA and SCA in context of modernizing workplace technologies).

327. *Konop*, 302 F.3d at 876–77; Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

328. *Konop*, 302 F.3d at 876–78; *Steve Jackson Games*, 36 F.3d at 463.

329. *See* 18 U.S.C. § 2701.

statute also contains sufficient exceptions such that employers can nearly always mount a ready defense to any employee's claim of its violation, either as the provider of the business's network services, or on grounds an employee user has in one fashion or another provided requisite statutory authorization to permit the employer access.[330]

The constrained interpretations that bound the first courts attempting to apply these antiquated statutes to modern technologies seem to be giving way to more protective interpretations in recent years. Thus, although the statutes remain outdated and cry out for revision, some courts have more recently found ways to afford greater protection to employees, even within the antiquated structure. An example of this phenomenon is *Steinbach v. Village of Forest Park*.[331] Plaintiff Steinbach was Commissioner of the Village of Forest Park, Illinois, an elected position.[332] When she then ran against the incumbent Mayor, she discovered that someone had accessed her Forest Park e-mail account and forwarded to the incumbent Mayor eleven e-mail messages she had received from her constituents.[333] Upon making this discovery, she sued the Village, its Mayor, and its IT employee, alleging various privacy-based claims.[334] The defendants responded with a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), but unlike the predecessor courts of the earlier era, the *Steinbach* court accorded the privacy claims a warmer reception.[335] Most relevant here is the court's interpretation of the relevant statutes. Although the court granted the defendants' motion to dismiss the claim that the plaintiff brought directly under the ECPA on grounds the Act did not apply to municipalities,[336] it relied on the Wiretap Act and SCA to support the plaintiff's common-law privacy claim.[337] Specifically, the defendants contended that plaintiff could not establish an "unauthorized" intrusion upon her seclusion because the Village was exempt from liability under the statute

330. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2003); *see also supra* Part I.B.2 (discussing *Fraser* and the SCA).

331. Steinbach v. Vill. of Forest Park, No. 06 C 4215, 2009 WL 2605283 (N.D. Ill. Aug. 25, 2009).

332. *Id.* at *1.

333. *Id.*

334. *Id.* at *1–2.

335. *Id.* at *2–7.

336. *Id.* at *2–3.

337. *Id.* at *4–5.

as a "provider," consistent with the first courts to interpret the statute in the context of e-mail.[338] The court, however, rejected that argument, instead interpreting the statute more forgivingly to the plaintiff's interests.[339] The court concluded that the third party from whom Forest Park purchased internet access—and not the city—was the "provider" under the statute, thus negating the city's exemption argument.[340] This novel interpretive approach facilitated success of plaintiff's common-law privacy claim where the narrower interpretations of the past would not. Moreover, because many, if not most, employers must purchase their network access from some third party, this line of reasoning has the potential to negate the employer's use of the "provider" exemption entirely.

Similarly, the court in *Pietrylo v. Hillstone Restaurant Group* also found a way around the statute via an employee-friendly interpretation.[341] As discussed above, the plaintiffs in *Pietrylo* sued their employer, the owner of the Houston's restaurant at which plaintiffs had worked; after they were discharged due to what Houston's deemed inappropriate content on a Myspace.com page.[342] Along with their common-law claims, discussed above, the plaintiffs also sued under the federal SCA and its state counterpart.[343] The defendant-employer was unable to take advantage of the "provider" exemption discussed above since the website was created remotely on the Myspace.com platform but argued against liability instead on grounds that access was authorized by a "user" of the service—a co-employee of the plaintiffs.[344] That co-employee had in fact provided her login information to her superiors,[345] but, like in *Steinbach*, the court nevertheless found a way around the statutory exemption. The fact that she may have felt pressure from her supervisors to share her access credentials in order to preserve her job created a fact question

338. *Id.* at *5; *see supra* Part I.B (discussing "early-era" interpretations of ECPA and SCA, which typically afforded a defense to employers as providers of network services).

339. *Steinbach*, 2009 WL 2605283, at *5.

340. *Id.*

341. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *3–4 (D.N.J. July 25, 2008).

342. *Id.* at *1; *see supra* notes 248–66 and accompanying text (discussing *Pietrylo*).

343. *Pietrylo*, 2008 WL 6085437, at *2.

344. *Id.* at *3.

345. *Id.* at *1.

concerning the effectiveness of the authorization she allegedly gave.[346] Summary judgment was therefore denied, and the statutory claim once again survived.[347]

2. Progressive Statutory Initiatives

While courts seem to be according more employee-friendly interpretations to the antiquated federal statutory framework, state legislatures are beginning to step into the fray as well by enacting new statutes that protect the privacy rights of the state's workforce. Indeed, worker privacy is a hot topic in state legislatures, as evidenced by the fact that thirty bills addressing some aspect of worker privacy were enacted in 2012 alone, adding new protections in twenty states.[348] The pervasiveness of legislative reform in the area of workplace privacy is further reflected by statistics showing that not only are many states considering such laws, but for the last two calendar years, state legislatures have enacted more laws concerning worker privacy than any other labor-related topic.[349]

A consistent theme in these state privacy enactments is limiting employer access to employee and applicant social-media accounts.[350] As social networking has become pervasive in recent years, concerns about worker privacy are moving beyond the classic e-mail-access scenario typified in the cases discussed above. Traditional privacy protections generally were not relevant to employee activity on social network sites, given their public nature, but employees nevertheless came to expect that their actions on social network sites were relevant only to their private lives outside of work, and therefore had no bearing on their jobs.[351] When it became more commonplace for

---

346. *Id.* at *4.

347. *Id.* at *7.

348. John L. Fitzpatrick, Jr. & James L. Perine, *State Labor Legislation Enacted in 2012*, MONTHLY LAB. REV., Feb. 2013, at 24, 29, *available at* http://www.bls.gov/opub/mlr/2013/02/art3full.pdf.

349. *Id.*; *see also States Targeted Worker Privacy, Trafficking in Labor Legislation Last Year, DOL Reports*, Daily Lab. Rep. (BNA) No. 43, at A-7 (Mar. 5, 2013) ("For the second consecutive year, the most legislative activity came in the worker privacy category, as 30 bills related to the subject were passed in 20 states during 2012. The latest figure comes after legislators enacted 31 privacy-related laws in 20 states a year earlier, as measured from Oct. 1, 2010, to Dec. 31, 2011.").

350. *See infra* notes 352–54 and accompanying text.

351. *E.g.*, Cathleen O'Connor Schoultz, *Workers, Employers See Privacy Differently; Good Mobile, Media Policy Can Close Gap*, Daily Lab. Rep. (BNA)

employers to request that employees and applicants turn over their social network login credentials, state legislatures responded by enacting laws prohibiting that practice. Maryland was the first state to pass such a law, but numerous other states have followed its lead.[352] Indeed, according to the National Conference of State Legislatures, six states enacted such laws in 2012,[353] ten more joined them in 2013, and such legislation had been introduced or was pending in at least thirty-six states by the end of the year.[354] Based on these statistics, it appears safe to say that such protections have become the norm, and that nearly every state may eventually grant them.

Some state legislatures have enacted other forms of privacy protections directed toward workers. For example, Connecticut and Delaware require that employers provide written notice to employees before monitoring employee e-mail or other Internet activities.[355] Colorado and Tennessee protect public employees' privacy by requiring that government entities adopt a written policy describing any electronic monitoring that may occur.[356] Thus, state legislatures are protecting the privacy rights of workers in the technological era with increasing frequency.

Federal law may not be far behind on the trajectory established by the states. The Password Protection Act of 2013, introduced in the House of Representatives on May 21, bears some similarity to the now-pervasive state laws restricting employer demands for social network passwords, but would

---

No. 56, at A-13 (Mar. 22, 2012) ("Employees tend to think they are in a private zone, especially if they are using their own mobile communication devices . . . .").

352. Kathy Lundy Springuel, *Maryland Is First State to Restrict Employer Demands for Employee, Applicant Passwords*, 85 Daily Lab. Rep. (BNA) No. 85, at A-12 (May 2, 2012); *see, e.g.*, Michael O. Loatman, *Washington Becomes Ninth State to Limit Employer Access to Social Media Accounts*, Daily Lab. Rep. (BNA) No. 100, at A-7 (May 23, 2013).

353. *Employer Access to Social Media Username and Passwords, 2012 Legislation*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (last visited Mar. 1, 2014).

354. *Employer Access to Social Media Username and Passwords*, *supra* note 228.

355. CONN. GEN. STAT. ANN. § 31-48d (West 2011); DEL. CODE ANN. tit. 19, § 705 (2005).

356. COLO. REV. STAT. § 24-72-204.5 (2008); TENN. CODE ANN. § 10-7-512 (2012).

reach even further by prohibiting employers from requesting a password to any computer.[357] A similar, narrower bill was introduced in 2012.[358] The Social Networking Online Protection Act was nearly identical to the statutes recently enacted in numerous states, and would have prohibited employers and universities from mandating access to employee/student e-mail accounts and social networking sites.[359] Of course, it remains unclear whether any such federal legislation will meet with success, but the mere fact that such bills have been introduced is itself indicative that legislative reform is possible. Likewise, although lying just beyond the scope of this Article due to its sweeping application beyond the workplace, it is nevertheless worth noting here that Congress is also considering revisions to the ECPA and SCA that would protect against warrantless e-mail searches by government authorities, thereby providing greater privacy protection to e-mail than the antiquated 1986 versions of the laws that currently remain in effect.[360] Other efforts to reform and update the "ancient" ECPA/SCA framework have thus far failed, but the recent flurry of state legislative activity in the electronic privacy arena suggests that

---

357. Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013); Ilyse W. Schuman, *Federal Bill Would Institute Social Media Password Protection*, MONDAQ (June 6, 2013), http://www.mondaq.com/unitedstates/x/243622/employee+rights+labour+relations/Federal+Bill+Would+Institute+Social+Media+Password+Protection ("Specifically, the bill would amend Section 1030 of Title 18 of the U.S. Code . . . to make it unlawful if an employer: 'for the purposes of employing, promoting, or terminating employment, compels or coerces any person to authorize access, such as by providing a password or similar information through which a computer may be accessed, to a protected computer that is not the employer's protected computer, and thereby obtains information from such protected computer.'").

358. Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

359. *Id.* § 2(a) ("It shall be unlawful for any employer . . . to require or request that an employee or applicant for employment provide the employer with a user name, password, or any other means for accessing a private email account of the employee or applicant or the personal account of the employee or applicant on any social networking website . . . .").

360. Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013); H.R. 1847, 113th Cong. (2013); *see also* Ryan Gallagher, *Ancient Electronic Communications Law May Finally Be Updated to Protect Email Privacy*, SLATE (Mar. 19, 2013, 4:08 PM), http://www.slate.com/blogs/future_tense/2013/03/19/patrick_leahy_introduces_legislation_to_update_ancient_electronic_communications.html.

more sweeping changes at the federal level may be lurking just around the corner.[361]

C. THE PRIVACY SPHERE CREATED BY ADMINISTRATIVE DECISIONS

Recent developments in the administrative-law arena also deserve mention as consistent with the theme toward greater recognition of employee rights in emerging technologies. Similar to the state legislation discussed above, the focus here lies in employee use of social media. As such, the issues that arise in this context do not implicate privacy in the traditional sense. But they are no less relevant as a result. The trends here, consistent with the judicial decisions, statutes, and legislation discussed above, reflect a theme favoring expansion of employee rights in modern technological platforms. The law implicated is the National Labor Relations Act (NLRA), and the protections it affords to employees who engage in "concerted activity"—i.e., group efforts to question or contest the terms and conditions of employment.[362] Social media presents opportunities for engaging in concerted activity that did not previously exist. These new forums give rise to novel legal issues, as employers attempt to discern the extent to which they can regulate employee conduct that may not occur in the physical workplace but nevertheless directly affects it. To that end, the National Labor Relations Board (NLRB) is fighting this battle on two related yet distinct frontiers—by challenging the propriety of disciplinary action taken against employees for their communications in social media settings, and by policing

---

361. Gallagher, *supra* note 360. Also consistent with the idea that Congress may be headed toward enactment of greater privacy protections for employees is a recent request by Republican lawmakers for a survey of e-mail monitoring policies applicable to federal workers. *See* Louis C. LaBrecque, *Republican Lawmakers Ask OMB for Survey of Federal Worker E-mail Monitoring Policies*, Daily Lab. Rep. (BNA) No. 44, at A-3 (Mar. 6, 2012).

362. *See* Hispanics United of Buffalo, Inc., 359 N.L.R.B No. 37, at 2 (2012) ("The Board first defined concerted activity in *Meyers I* as that which is 'engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself.' 268 NLRB at 497. In *Meyers II*, the Board expanded this definition to include those 'circumstances where individual employees seek to initiate or to induce or to prepare for group action, as well as individual employees bringing truly group complaints to the attention of management.'"). *See generally* 29 U.S.C. § 157 (2012) ("Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection . . . .").

the content of employer policies that might be construed as regulating such communications.[363] The NLRB has decided one representative case in each of these categories; together, they paint a clear picture of the state of the law in this arena.

The NLRB's decision in *Hispanics United of Buffalo, Inc.* perfectly illustrates the hazards of taking disciplinary action against employees who communicate with each other about their jobs in a social media setting.[364] Hispanics United employee Mariana Cole-Rivera posted to her Facebook page, during non-working hours: "Lydia Cruz, a coworker feels that we don't help our clients enough at [work]. I about had it! My fellow coworkers how do u feel?"[365] Four other employees, none of whom were working at the time, responded, each generally objecting to the suggestion that they were not doing a good job.[366] When the Executive Director of the organization learned about these Facebook postings, she terminated their employment.[367]

One of the discharged employees filed a charge under the NLRA, contending that the termination of his employment constituted an unfair labor practice.[368] The General Counsel then issued a complaint, alleging that the employees' termination violated the NLRA's prohibition against discouraging concerted activities.[369] The administrative law

---

363. *See*, *e.g.*, *Hispanics United*, 359 N.L.R.B. No. 37 (evaluating unfair labor practice charge alleging that employer improperly discharged four employees who objected, via Facebook comments, to a suggestion that their supervisor found their work to be substandard); Costco Wholesale Corp., 358 N.L.R.B. No. 106, at 1 (2012) (affirming finding of administrative law judge (ALJ) that employer's written policy prohibiting electronic communications that "damage the company" unlawfully inhibits protected concerted activity); *see also* Karl Knauz Motors, Inc., 358 N.L.R.B. No. 164, at 1 (2012) (affirming finding of ALJ that employer's "courtesy" rule, prohibiting disrespectful conduct and "language which injures the image or reputation of the Dealership," unlawfully prohibits protected concerted activity).

364. *See Hispanics United*, 359 N.L.R.B. No. 37.

365. *Id.* at 2.

366. *Id.*

367. *Id.*

368. *Id.* at 6; *see also id.* at 8 ("Section 8(a)(1) provides that it is an unfair labor practice to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7. Section 7 provides that, 'employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, *and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection* . . . .'").

369. *Id.*

judge (ALJ) upheld the charge, concluding that the employees were discharged unlawfully for engaging in protected concerted activity:

> Employees have a protected right to discuss matters affecting their employment amongst themselves. Explicit or implicit criticism by a coworker of the manner in which they are performing their jobs is a subject about which employee discussion is protected by Section 7. That is particularly true in this case, where at least some of the discriminatees had an expectation that Lydia Cruz-Moore might take her criticisms to management. By terminating the five discriminatees for discussing Cruz-Moore's criticisms of HUB employees' work, Respondent violated Section 8(a)(1).[370]

On review, the NLRB affirmed the ALJ's findings.[371] Like the ALJ, the Board found no reason to depart from otherwise-applicable precedents solely on the basis that the mode of communication—Facebook—was novel.[372] Finding that the employees' comments were protected concerted activity, the Board therefore upheld the ALJ's conclusion that their discharge was unlawful.[373]

An employer's knee-jerk response to the *Hispanics United* decision might be to publish a policy broadly prohibiting negative comments about the employer on social media, in order to avoid the scenario that ultimately transpired in that case. Such an approach would not be advisable, however, in light of the other frontier on which the NLRB is attacking employer regulation of employee social-media use. In *Costco Wholesale Corp.*,[374] the other seminal NLRB decision addressing social media in 2012, the Board concluded that an employer violated section 8(a)(1) of the NLRA when it published and enforced a policy prohibiting electronic communications "that damage the Company, defame any individual or damage any person's reputation, or violate the policies outlined in the [company's employee agreement]."[375] Rejecting the ALJ's contrary finding, the Board found that "employees would reasonably conclude that the rule requires them to refrain from engaging in certain protected

370. *Id.* at 9.

371. *Id.* at 1.

372. *Id.* ("Although the employees' mode of communicating their workplace concerns might be novel, we agree with the judge that the appropriate analytical framework for resolving their discharge allegations has long been settled . . . .").

373. *Id.*

374. Costco Wholesale Corp., 358 N.L.R.B. No. 106 (2012).

375. *Id.* at 1.

communications."[376] In other words, because the policy might chill employee speech falling within the protections of the Act as concerted activity, the policy was itself unlawful. As such, not only must employers guard against disciplining employees who use social media to communicate with coworkers about the terms and conditions of their employment, but they also must ensure that such communications are neither prohibited nor discouraged. The result is that employers are limited in their ability to regulate employee use of social media, thereby at least suggesting that employees retain some notion of privacy in their use of social media during non-working hours, even when such use pertains directly to their job.

III. JUXTAPOSING THE TRENDS AND HYPOTHESIZING FROM THEIR TRAJECTORY

There can be no doubt that the law of employee privacy in workplace technologies is shifting as social norms evolve. The first courts to confront issues of employee privacy in emerging technologies evinced grave trepidation about creating any new rights, clinging firmly to rudimentary conceptions about how such technologies worked.[377] As the first decade of the new millennium drew to a close, though, the tide appeared to turn.[378] Courts no longer expressed such disdain for claims of privacy in workplace technologies, instead opening wider the court house doors, inviting more plaintiffs in.[379] All this transpired in spite of the early-era precedents to the contrary, and often in the face of employer policies attempting to take the wind out of such claims' sails even before they could take flight. As technology use became increasingly pervasive, social norms shifted to reflect that change.

The preceding detailed exposition of the cases that typified the "early" and "modern" eras of technology-based employee privacy reveals in lucidity the unmistakable shift in the legal response to such claims. In case of any lingering doubt, though, a few direct comparisons should quiet any naysayers. And, while the trends of the past and present might inform us about how far we have come, they do not obviate the path of the future. This Part endeavors, therefore, to solidify the stark

376. *Id*. at 2.

377. *See supra* Part I.A.1 (discussing trepidation of early-era courts).

378. *See supra* Part II.A.1 (discussing a trend toward greater recognition of employee rights in the modern era).

379. *See supra* Part II.A.1.

contrast of the trends established in Parts I and II by directly juxtaposing certain early cases against comparable modern ones. It then proceeds to draw conclusions about what all of this means for what is otherwise a most assuredly uncertain future.

A. A COMPARATIVE JUXTAPOSITION

Juxtaposition of the trends identified in the preceding Parts of this Article reveals in stark fashion a shift from reluctance to acceptance in the law of employee privacy rights. When technologies were new, courts were extraordinarily reticent to carve out or establish employee rights. But as technologies have undergone rapid expansion and growth and their usage has become more commonplace, so that even the very judges and legislators leading the law's development are using these technologies on a daily basis, the reality of the shifting social norms can no longer be ignored. A few direct comparisons best illustrate this point.

The first illustrative example juxtaposes the earliest published case addressing employee privacy rights in e-mail against one of the starters of the modern revolution. Recall *Smyth v. Pillsbury Co.*,[380] and *Pure Power Boot Camp v. Warrior Fitness Boot Camp*.[381] Both cases addressed the privacy rights of employees in e-mail, and in both cases, the employer either made assurances or published a policy purporting to establish (or defeat, as the case may be) those rights.[382] The contrast between the employers' approaches is alone striking, but the juxtaposition becomes even more glaring in light of the decisions the courts made about the employees' privacy. In *Smyth*, the employer repeatedly assured its employees that all e-mail communications were confidential and that they "could not be intercepted and used by [the employer] against its employees as grounds for termination or reprimand."[383] Notwithstanding these assurances, the court concluded that employees could not and should not expect any

---

380. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); *see supra* notes 45–82 and accompanying text (discussing *Smyth*).

381. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008); *see supra* notes 230–47 and accompanying text (discussing *Pure Power Boot Camp*).

382. *Pure Power Boot Camp*, 587 F. Supp. 2d at 552–53; *Smyth*, 914 F. Supp. at 98–100.

383. *Smyth*, 914 F. Supp. at 98.

privacy in their e-mail communications.[384] Indeed, the court reached this conclusion with very little analysis, finding "no privacy interests in such communications."[385]

Pure Power Boot Camp, decided twelve years later, stands in stark contrast. The employer there took the opposite approach, expressly and directly negating any expectations of privacy in employees' computer communications via a policy published in the Employee Handbook: "[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*."[386] Notwithstanding that policy, however, the court concluded that the employees in that case *could* expect privacy in the e-mail messages they sent on their personal web-based e-mail accounts, even though they had not only accessed those accounts from company equipment but had also stored their login credentials there, permitting ready access by anyone who could get to the computer.[387]

The contrast between these two cases boldly exemplifies the shift that has occurred from the early era of workplace privacy in emerging technologies, to the modern era of pervasive and highly developed technology use. The *Smyth* court, refusing even to engage a discussion about what the employee legitimately or reasonably might have expected in using his company e-mail, leaped quickly to the conclusion that no privacy interests existed, despite the employer's assurances to the contrary.[388] The court's approach evinces great trepidation at the idea of establishing privacy rights, and perhaps that reluctance is attributable, at least in part, to the relative novelty of the e-mail medium at that time. In 1996, e-mail had just begun to be a pervasive mode of communication in American workplaces.[389] The judge who decided the *Smyth*

---

384. *Id.* at 101.

385. *Id.*

386. *Pure Power Boot Camp*, 587 F. Supp. 2d at 552 (emphasis omitted).

387. *Id.* at 561 ("There is no sound basis to argue that [employee], by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts.").

388. *See Smyth*, 914 F. Supp. at 101.

389. *See* Rob Spiegel, *When Did the Internet Become Mainstream?*, E-COMMERCE TIMES (Nov. 12, 1999, 12:00 AM), http://www.ecommercetimes.com/story/1731.html (last visited Aug. 21, 2013)

case may well have had little or no experience with it himself. That inexperience, in turn, could have contributed to his swift conclusion that it is unreasonable to expect privacy in e-mail—a conclusion that is all the more remarkable given that the employer had, at least as alleged by the plaintiff, "repeatedly assured its employees, including plaintiff, that all e-mail communications would remain confidential and privileged."[390]

The evolution of social norms in the face of rapidly expanding use of technology in the workplace over the twelve years that intervened between *Smyth* and *Pure Power Boot Camp* may well explain the polar opposite result reached in the later case. Quite unlike Pillsbury, the employer in *Pure Power Boot Camp* expressly and unequivocally declared in a published handbook policy that employees should *not* expect privacy in their computer communications and activities.[391] Yet, the court still found that the employee's privacy expectations were reasonable.[392] The fact that the employee sent the subject e-mail over his personal, web-based e-mail account, as opposed to the e-mail account provided by his employer, may have made a difference in this aspect of the court's determination. However, the employee also saved his login credentials on his company computer, effectively leaving the key in the door and facilitating ready access to his otherwise-personal account.[393] Even so, the court still found that the employee could expect privacy.[394] Shifting social norms may explain this result. By 2008, e-mail use had become much more pervasive, and it was not uncommon for employees to use it frequently for both professional and personal purposes.[395] Social norms had shifted, and the courts seemed to be tracking those changes.

Other comparisons also illustrate the turn of the tide away from the disdain expressed in the early era and toward the acceptance of privacy rights in the modern era. The plaintiff in *McLaren v. Microsoft Corp.*, another early-era case, went so far

---

("Twelve months ago, I never would have predicted that Internet usage would become completely mainstream by November 1999.").

390. *Smyth*, 914 F. Supp. at 98.

391. *Pure Power Boot Camp*, 587 F. Supp. 2d at 552.

392. *Id.* at 560.

393. *Id.*

394. *Id.*

395. *See generally* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 654 (N.J. 2010) ("In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail.").

as to protect the "personal" e-mail folder on his work computer with a password that only he knew on a system devised and provided by his employer.[396] McLaren argued that the law should not treat his password-protected e-mail folder any differently than it treated a locked locker in the pre-technological era.[397] The court, however, cast aside the password as essentially irrelevant, concluding instead that because the e-mails were transmitted over the company system, McLaren could expect no privacy in them, password or not.[398] The court's decision reflects, therefore, a grave reluctance to recognize any privacy rights in emerging technologies.

The *McLaren* court's reticence becomes clearer when viewed in contrast to the somewhat comparable scenario in *Pure Power Boot Camp*, which netted an opposite result. As discussed above, the court in *Pure Power Boot Camp* found that the employee could reasonably expect privacy in the e-mail messages sent from, received on, and stored in his personal web-based e-mail account, even though he had accessed that account from his employer's computer *and* had gone so far as to save his login credentials there, providing ready access.[399] Despite having readily enabled such access, the court still concluded that the employee could reasonably expect privacy in the account's contents.[400] This result therefore stands in stark contrast to that of *McLaren*, in which the court swiftly rejected the plaintiff's privacy claims, even though he had protected his e-mail with a password. In other words, the early-era employee who password-protected his account could not expect privacy, but the modern-era employee who enabled ready access by saving his password on the computer could.

Yet another juxtaposition, comparing the courts' reception to traditional causes of action as vehicles for supporting novel privacy rights, makes the point here even more emphatically. As discussed in Part I above, many of the earliest plaintiffs to pursue vindication of privacy rights in emerging workplace technologies sought to establish claims under the existing

---

396. McLaren v. Microsoft Corp., No. 05-97-00824, 1999 WL 339015, at *5 (Tex. App. May 28, 1999).

397. *Id.* at *4 (discussing K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. App. 1984)).

398. *Id.*

399. *Pure Power Boot Camp*, 587 F. Supp. 2d at 559–60.

400. *Id.*

common-law framework.[401] Indeed, the plaintiffs in nearly every seminal early-era case discussed in Part I sought relief at least in part on a common-law tort theory like invasion of privacy, wrongful discharge in violation of public policy, or both.[402] Each and every such plaintiff failed in that endeavor, with the overwhelming majority of the courts swiftly rejecting their claims on grounds that no reasonable expectation of privacy existed, thereby tolling the death knell of their common-law claims, no matter what the underlying theory.[403]

In the modern era, by contrast, courts became increasingly receptive to such claims. For example, the plaintiff's claims in *Steinbach v. Village of Forest Park* bore several striking resemblances to the claims brought by the early-era trailblazers.[404] Like her predecessors, Steinbach sued for invasion of privacy, asserting both common-law and statutory theories.[405] Unlike the prior courts, though, this one denied the defendant's motion to dismiss, concluding that the law *could* support Steinbach's privacy claims on the facts she had alleged.[406] The wariness that led the early-era courts to dismiss

---

401. *See supra* Part I.A.1 (discussing the earliest cases in which plaintiffs brought common-law privacy claims).

402. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 111, 116 (3d Cir. 2003) (considering plaintiff's claims for wrongful termination and invasion of privacy); Garrity v. John Hancock Mut. Life Ins. Co., No. Civ.A. 00-11243-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002) (discussing plaintiffs' invasion of privacy claim); Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1997) (discussing plaintiff's claim for wrongful discharge in violation of public policy); Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html (addressing plaintiffs' claims for common-law invasion of privacy and wrongful discharge in violation of public policy); McLaren v. Microsoft Corp., No. 05-97-00824, 1999 WL 339015, at *4–5 (Tex. App. May 28, 1999) (addressing plaintiff's invasion of privacy claims). *See generally supra* Part I.A (discussing cases cited hereinabove).

403. *See Fraser*, 352 F.3d at 111–13 (affirming summary judgment to employer on plaintiff's wrongful discharge claim because no public policy was implicated due to absence of protectable privacy right); *Garrity*, 2002 WL 974676, at *1–2 (dismissing invasion of privacy claim on grounds of no reasonable expectation of privacy in e-mail); *Smyth*, 914 F. Supp. at 100–01 (granting motion to dismiss wrongful discharge in violation of public policy claim upon finding employee could not reasonably expect privacy in e-mail); *Bourke*, No. B068705 (concluding that plaintiffs lacked reasonable expectation of privacy in e-mail and rejecting invasion of privacy and wrongful discharge claims on that basis); *McLaren*, 1999 WL 339015, at *4 (same).

404. Steinbach v. Vill. of Forest Park, No. 06 C 4215, 2009 WL 2605283, at *1–5 (N.D. Ill. Aug. 25, 2009).

405. *Id.* at *2.

406. *Id.* at *4.

before the claims ever left the starting gates therefore gave way to not just a willingness but indeed a genuine interest in allowing the claims to proceed.

Similarly, the court in *Pietrylo v. Hillstone Restaurant Group* also accorded the plaintiffs' invasion of privacy and wrongful discharge claims a much warmer reception.[407] Indeed, the court in *Pietrylo* confronted essentially the same question that led to the demise of most early-era claims—whether a right to privacy could support a wrongful discharge claim as a relevant source of public policy.[408] Its answer, however, was markedly different. The court stated quite plainly that "[a] right to privacy may be a source of 'a clear mandate of public policy' that could support a claim for wrongful termination."[409] Based on that conclusion, the court denied the defendant's motion for summary judgment, finding that the plaintiffs reasonably expected privacy in their invitation-only website, and that a genuine fact issue existed concerning whether the employee who granted management access did so voluntarily.[410]

The change of course in modern-era treatment of common-law claims provides further support for the theory espoused here, that shifting social norms have facilitated an evolution in the law, as courts have accorded increasingly broader privacy rights in workplace technologies. The role that social norms play in this process, however, becomes more evident in light of the express recognition by some courts of their significance. For instance, in *Pietrylo*, not only did the court break new ground in accepting a right to privacy as a sufficient source of public policy, but the court also stated expressly that "expectations of privacy are established by general social norms."[411] Similarly, the court in *Stengart v. Loving Care Agency, Inc.*, on the way to finding that the plaintiff could reasonably expect privacy in e-mail communications with her lawyer through a personal web-based account accessed on company equipment, concluded that social norms play a vital role in the establishment of the law in

---

407. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008).

408. *Id.* at *6.

409. *Id.*

410. *Id.*

411. *Id.* at *7 (quoting White v. White, 781 A.2d 85, 92 (N.J. Super. Ct. Ch. Div. 2001)).

this arena.[412] To that end, the court began its opinion with an expression about the impact of social norms on workplace rights:

> In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur.
>
> In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.[413]

Those evolving social norms then proved integral in the court's conclusion that the plaintiff's privacy expectations were reasonable, notwithstanding an employer policy attempting to defeat any such expectancy.[414]

The Supreme Court's most recent instruction about workplace privacy in modern technologies, notwithstanding its failure to answer open questions about the governing law, also illustrates that social norms play a vital role in the shaping of that law.[415] Indeed, the majority touted the evolution of social norms, and the speed with which the evolution proceeds, as the primary justification for its refusal to reach any firm conclusions about the law governing employees' privacy expectations:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear . . . . Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.[416]

---

412. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 654 (N.J. 2010).

413. *Id.* at 654–55.

414. *See id.*

415. *See* City of Ontario v. Quon, 560 U.S. 746, 758–61 (2010).

416. *Id.* at 759.

It was this very reluctance to make any firm declarations about the law of workplace privacy expectations that elicited a scathing response from Justice Scalia in his concurrence:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would . . . —or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible.[417]

And thus Justice Scalia returns us to the point at which this Article began, with a reference to the prophetic lyrics of Bob Dylan: "The-times-they-are-a-changin' is a feeble excuse for disregard of duty."[418]

B. THE TRAJECTORY OF THE FUTURE

Having firmly established that shifting social norms are turning tides in the law of employee privacy, the question remains: What next? Indubitably, new technological frontiers that we cannot yet fathom will raise novel issues repeatedly in the years to come. Some of these frontiers have already been discovered but remain relatively unexplored. Examples include online social media, and the use of GPS devices to track employee whereabouts and habits.[419] How the law should respond to these burgeoning frontiers remains in some doubt, but the recent evolution in the law suggests at least two possible approaches. Because this Article takes a comparative-retrospective approach, exposing the shift in trends that has occurred over the past quarter century, a full exposition and hypothesis on how the law should ultimately resolve this quandary in the future is beyond its scope. Nevertheless, some excursus on the prospects is appropriate.

The first possible approach is that espoused by the majority of the Supreme Court in *City of Ontario v. Quon*.[420]

---

417. *Id.* at 768–79 (Scalia, J., concurring) (citation omitted).

418. *Id.* at 768.

419. *See generally* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 473–74 (N.Y. 2013) (holding that GPS tracking of state employee's car did not require a search warrant under what the court termed the "workplace exception," but finding the search unreasonable due to continuation during non-working hours); Joyce E. Cutler, *Companies Should Inform Workers of Risks with Social Media, LinkedIn Counsel Advises*, Daily Lab. Rep. (BNA) No. 135, at A-9 (July 15, 2013) (discussing rising prominence of social media use in workplace).

420. *Quon*, 560 U.S. at 758–61.

Much akin to the early-era courts, the majority in *Quon* evinced reluctance and grave trepidation about charting any new course in the law of workplace privacy given the rapid maturation of relevant social norms.[421] Having gone to great pains to avoid broaching that subject, though, the Court has in effect declared a piecemeal approach.[422] Without direct instruction from the Supreme Court, litigants and judges are left to determine, based on the scattered precedents, what the law should be and how it should (or should not, as the case may be) respond to social change. This approach has the appeal of malleability, permitting the development of the law to track society's progression. But it is not without its shortcomings, chief among which are ambiguity and lack of predictability.

The alternative approach might avoid some of these pitfalls, but is also not without imperfections. Justice Scalia, dating back to the Court's early forays into the law of workplace privacy, well before the advent of modern technology, has long espoused the view that subjectivity in this arena is undesirable.[423] According to Justice Scalia, subjectivity only breeds ambiguity.[424] The law should therefore assume categorically, he suggests, that privacy interests exist, obviating the need for inquiry into subjective expectations.[425] The inquiry therefore need only focus on whether the subject search was itself reasonable.[426] The appeal of Justice Scalia's categorical approach lies in its relative simplicity. Quite obviously, a standard that resolves upon only a single inquiry is simpler than a two-step analysis. It is that very

---

421. *Id.*

422. *Id.*; *see id.* at 768 (Scalia, J., concurring) ("Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described 'instructive' expatiation on how the *O'Connor* plurality's approach would apply here (if it applied), as a heavy-handed hint about how *they* should proceed." (citation omitted)).

423. *Id.* at 767–68 (discussing O'Connor v. Ortega, 480 U.S. 709, 717 (1987)).

424. *Id.*; *see also O'Connor*, 480 U.S. at 730 (Scalia, J., concurring) ("Even if I did not disagree with the plurality as to what result the proper legal standard should produce in the case before us, I would object to the formulation of a standard so devoid of content that it produces rather than eliminates uncertainty in this field.").

425. *O'Connor*, 480 U.S. at 730–32 (Scalia, J., concurring).

426. *Id.*; *see also Quon*, 560 U.S. at 767 (Scalia, J., concurring) ("I continue to believe that the 'operational realities' rubric for determining the Fourth Amendment's application to public employees invented by the plurality in *O'Connor v. Ortega* is standardless and unsupported." (citation omitted)).

simplification, however, that casts some doubt upon its efficacy and appropriateness. If the detailed exposition in Parts I and II above reveals nothing else, it shows that nothing is static in the law of workplace privacy. Given the continuing rapid expansion of technology and its direct impact on the workplace, it may be naive, if not improper, to make the kind of assumptions that Justice Scalia's categorical approach requires. And whatever the benefits and shortcomings of these alternate approaches may be, it remains clear that no obvious solution has emerged. The law continues to evolve along with the social norms, though, and perhaps that perfect answer lies just around the next bend.

CONCLUSION

No one can deny that when it comes to the law of employee privacy in workplace technologies, the times they are a-changin'. In the early era of technology in the workplace, courts demonstrated great reluctance to carve out any ambit of protection. Almost without exception, the early courts concluded summarily that employees had no right of privacy whatsoever in electronic communications. The common law therefore afforded no relief to aggrieved employees, and the antiquated statutes that purport to govern such issues offered little respite as well.

Over the course of the last decade, though, social norms have begun to shift as the use of technology has become increasingly pervasive both in the workplace and beyond. The law may not have kept pace, but it is certainly evolving. Although the antiquated statutes remain a sole source of protection at the federal-law level, states are responding by recognizing common-law protections for privacy rights that did not previously exist and enacting new legislation addressed to specific privacy concerns. Thus, as society itself becomes more immersed in modern modes of communication, the law is beginning to recognize that traditional notions of privacy may no longer apply. The trajectory of the future is uncertain, but if any lesson can be gleaned from the experience of the last quarter century, it is that when it comes to privacy interests in constantly-changing workplace technologies, the law must either begin to anticipate changes or remain flexible to respond rapidly. The course of the future is yet unknown, but it is certain that it includes progress that the law must address.

***