BIT-WISE BUT PRIVACY FOOLISH: SMARTER E-MESSAGING TECHNOLOGIES CALL FOR A RETURN TO CORE PRIVACY PRINCIPLES

John Soma, Melodi Mosley Gates, & Michael Smith[*]

TABLE OF CONTENTS

[*] John Soma is a professor of law at the University of Denver Sturm College of Law and the Executive Director of the Privacy Foundation. Melodi Mosley Gates is a December 2010 J.D. candidate who was previously the chief information security officer for a large telecommunications organization. Michael Smith, J.D., University of Denver Sturm College of Law, served as the Editor-in-Chief of the *Denver University Law Review* in 2008–09.

I. INTRODUCTION

In this era of constantly evolving electronic messaging ("e-messaging") features and functions, courts have unfortunately been seduced by the glow of individual technologies. As we will demonstrate, rather than calling for unique treatment, each of these technologies serve as simply another means to support interpersonal communications and cry out for consistent policymaking. Failing to grasp this overarching and functional perspective, courts have fallen down a rat hole of technical idiosyncrasies, thereby missing the opportunity to apply core privacy principles in a technology-agnostic manner. Instead of a consistent set of policies and user rights, we are left with an incoherent mix of varying rights, obligations, and rulings based on the technology of the day. Moreover, technology continues to evolve and complexities only increase, thus creating more uncertainty.

Now is the time for policymakers and service providers to regroup, cooperate, and address e-messaging consistently—from a user's perspective—by applying the core privacy principles our judiciary recognized so early in the technology age. Otherwise, the hope for coherency and consistency in privacy policy will fade even further with each new technology that emerges, thus leaving the employers and employees who most benefit from these technologies in the dilemma of whether to risk legal uncertainty or leverage e-messaging's promise of enhanced productivity.

In their groundbreaking article, Samuel D. Warren and Louis D. Brandeis recognized the need to preserve core privacy principles, especially in the midst of emerging technologies.[1] While the advent of the news media and "instantaneous photographs" troubled them, today's many forms of e-messaging create an always-on, always-present means of digitizing and recording every aspect of our lives.[2] These innovative-messaging technologies give us new features, functions, and capabilities, but

[1] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

[2] *Id.* at 195; *see* Eleanor Dallaway, *The Whole World is an Airport Security Area, Says Schneier*, INFO SECURITY, Nov.-Dec. 2008, at 10, *available at* http://e-ditionsbyfry.com/Olive/AM3/IST/Default.htm?href=IST%2F2008%2F12%2F01&pageno=12&entity=Ar01200&view=entity (stating that information from everyday technology such as cell phones and GPS is saved without our knowledge).

current law and regulatory approaches, as well as service provider practices regarding electronic messaging and privacy, are disparate and confusing. Even technology experts have called for clearer rules in this new game, in no small part because those "[w]ho control[] our data control[] our lives."[3]

Complicating matters are converging technologies that require multiple regulatory agencies to be involved. For example, individuals may now engage in conversations using at least five different means on their mobile devices.[4] While the FCC regulates telephone carriers and Internet service providers, increasingly, the FTC regulates e-commerce and the websites used to exchange messages.[5] Consequently, this results in a disjointed regulatory approach lacking the cohesion and consistency desired by consumers. Adding to the challenges of a coherent regulatory approach are new "Web 2.0" technologies[6] that allow users to share information at deeper levels across a variety of services and applications, while simultaneously providing more e-messaging capabilities—think Facebook and MySpace.[7]

---

[3] BRUCE SCHNEIER, SCHNEIER ON SECURITY 61 (Wiley Publ'g Inc., 2008). *See* Dallaway, *supra* note 2, at 10 ("Just because a technology exists, it doesn't have to be used to its fullest. Privacy is a balancing act and information technology is changing that balance. Where technology can't save us, laws tend to step in.") (quoting Schneier).

[4] *See, e.g.,* AT&T, Messaging, http://www.wireless.att.com/learn/messaging-internet/messaging/ (last visited Apr. 25, 2010) (discussing how AT&T mobile devices allow individuals to text cell phones and email addresses, converse using group messaging, chat with instant messaging, and exchange pictures and live stream video).

[5] *See* Kevin Werbach, *Off the Hook*, 95 CORNELL L. REV. 535, 537–38, 540, 549–50 (2010) (describing the jurisdiction of the FCC); NetSafekids, Regulatory Agencies: The FTC and FCC, http://www.nap.edu/netsafekids/pp_li_ra.html (last visited Apr. 20, 2010) (describing the jurisdiction of the FTC); *see, e.g.,* Federal Trade Commission, FTC Business Information - E-Commerce, http://www.ftc.gov/bcp/menus/business/ecommerce.shtm (last visited Apr. 25, 2010) (providing various e-commerce resources for aiding consumers and businesses online).

[6] The term Web 2.0 was first used by Tim O'Reilly. *See* Tim O'Reilly, What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, O'REILLY MEDIA, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (describing web-based services that encourage user-created content such as social networking and other interactive sites, taking the web beyond its first generation (1.0) rendition that was primarily geared to one-way information delivery rather than collaborative content creation).

[7] *See id.*; *see also* Nicholas Kolakowski, *Microsoft Announces Facebook, MySpace Partnerships for Outlook*, EWEEK.COM, Feb. 17, 2010, http://www.eweek.com/c/a/Windows/Microsoft-Announces-Facebook-MySpace-Partnerships-

The goal of this Article is to lay out a regulatory prescription for confronting these new problems with an emphasis on protecting consumer privacy without encumbering service providers in delivering high-quality access to e-messaging services. We argue that the government should regulate matters of privacy in the same way, whether related to online or offline issues.[8] Both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) regulate Internet and online communications issues;[9] and given this overlap the agencies should engage in joint rulemaking to ensure online communications privacy is regulated in a comprehensive, consistent manner.[10] Joint rulemaking will provide more cohesion across the agencies and offers service providers and consumers the consistency and predictability necessary for a more efficient marketplace and privacy protections.[11]

The Article begins by discussing how new technologies can increase the vulnerability of both employees and employers. We then discuss the primary technologies that contribute to the vulnerability as well as the competing interests of all the major players in this area. After a brief discussion of some further considerations we address current law on privacy and protection. We then propose how to best achieve balance in this area with emphasis on a regulatory approach consisting of joint rulemaking by the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC). We also discuss ways that service providers could contribute to the solution.

II. THE PROBLEM: NEW TECHNOLOGIES MAKE EMPLOYEES AND EMPLOYERS VULNERABLE

With all these exciting new techno-advantages come some legal realities, and the "law has always been slow to catch up with technological advances . . . ."[12] For a general example, we need

for-Outlook-299131/.

[8] *See generally* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 158–60 (2002) (concluding there are nine key policy developments needed in online privacy).

[9] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1679–80 (1999).

[10] *See* discussion *infra* Part V.

[11] *See id.*

[12] Joshua A. Hawks-Ladds & Megan M. Youngling, Do PDAs Create Unlimited Wage Exposure from Nonexempt Employee Use? (Jan. 15, 2009) (unpublished manuscript, on file with the Albany Law Journal of Science &

look no further than our own backyard where in "the United States and most industrialized countries, private and public sector employers are purchasing and implementing new advanced technologies that enhance the monitoring of security and productivity while substantially increasing the level of intrusion into employee privacy."[13] Employers reason that they have the right to closely monitor their employees, "as a managerial prerogative aimed at increasing efficiency, tracking employees, and monitoring employer-owned property."[14] This type of workplace surveillance will surely have (or already has) a chilling effect on employee attitudes. After all, we are already vigilantly on the lookout for "Big Brother" in the public sphere; now, many citizens have to monitor his presence in the workplace.[15]

Technology and online), *available at www.ctemploymentlawblog.com/uploads/file/bb.DOC*.

[13] William A. Herbert & Amelia K. Tuminaro, *The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?*, 25 HOFSTRA LAB. & EMP. L.J. 355, 355 (2008). This article was part of a Symposium entitled "Emerging Technology & Employee Privacy" and it focused primarily on issues related to the use of new technologies and surveillance of employees. This is not the issue we are tackling in the current paper, but it does provide a good background discussing the impact of new technologies on employees. *See id*. at 355–58.

[14] *Id.* at 356. Prior to law school, one of the authors of this article worked in a residential treatment center for emotionally and behaviorally disturbed children and youth. There were enormously challenging problems related to incidents of aggression by the youth, and there was some reason to believe that much of the behavior was provoked by some of the staff members. After months of failed attempts at handling this issue in other less intrusive ways, the decision was made to implement video-monitoring equipment throughout the facility. To make a long story short, this may have solved one problem, but it created many more. The directors of the treatment center had 24/7 visual access to the employees and residents and this resulted, quite frankly, in some perceived abuses of the technology. Staff members could easily be singled out for various infractions (sometimes small, sometimes large), and the cameras could be—and often were—used to turn small, manageable issues into large and morale-busting affairs. The overall experience suggested that the cameras created bigger problems than they solved and were thus a net loss to the operation of the facility. This could be the result of many other factors that were germane to this particular facility but the broader point is still valid: Technologies that seem to make life easier often end up doing just the opposite.

[15] Simply visit Google.com and enter such search terms as "employee privacy, email monitoring, European Union" to get an idea of the concerns. *See also* John Wagley, *EU Balks at Employee Monitoring*, SECURITY MANAGEMENT, Oct. 2009, http://www.securitymanagement.com/article/eu-balks-employee-monitoring-006229 (discussing the EU's distaste for employee monitoring and the alternative provided by anonymization and masking techniques such as those in DLP). The approach suggested by the quoted attorneys is the same as the

But some commentators argue that it is reasonable to allow employers some latitude in policies related to these issues—that employees often take advantage of employers and thereby cause harm to a larger group in the workplace. Regardless of the motives, there is increasing evidence that "employers often ignore the adverse consequences to employee morale and occupational health" and that the introduction of new technologies that enhance the opportunity for surveillance "can lead to stress, alienation, and dehumanization of the workforce, resulting in unintended decreases in worker productivity and job satisfaction."[16]

More specifically, "[o]veruse of e-mail and portable communication devices containing tracking technology, such as BlackBerrys, can intensify work related stress and anxieties."[17] This has become such a problem that mental health professionals have begun to take notice of the reliance some people have towards their personal technological devices. A Harvard psychiatrist has even coined the phrase "acquired attention deficit disorder [that] describe[s] a psychological disorder resulting from the addictive qualities associated with the use of various communication devices such as BlackBerrys."[18]

The impact of technology on the workplace has a long history, but there is a new breed of technologies that are imposing new challenges and the correct response by employers and lawyers that represent them is anything but obvious. The Blackberry has been around for about ten years, which is remarkably new technology compared to things like cell phones and pagers (which seem quite rare these days). Consequently, we do not yet know

one we suggest in leveraging new technologies to balance interests. Despite the cultural differences, European countries struggle with the same balancing needs as shown by Finland's recent acquiescence to permit employee email monitoring by one of its major employers. *See, e.g.,* Pertti Jokivuori, *Nokia Wins Company Right to Monitor Employee E-mails*, EIRONLINE, Mar. 31, 2009, http://www.eurofound.europa.eu/eiro/2009/02/articles/fi0902059i.htm. *See also* Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829, 831–32 (2005) (contrasting American and European employer practices); *see also* OUT-LAW.COM, EU Court Rules Monitoring of Employee Breached Human Rights, REGISTER, Apr. 5, 2007, http://www.theregister.co.uk/2007/04/05/monitoring_breached_human_rights/.

[16] Herbert & Tuminaro, *supra* note 13, at 356.

[17] *Id*. The article goes on to tell of a situation in April 2007 when there was a lengthy disruption in Blackberry service which resulted in "paranoia among some Blackberry users." *Id*.

[18] *Id*. at 356–57.

"the adverse impact of sophisticated . . . technology on both employees and supervisors . . . ."[19]

It seems rather obvious that these technologies are here to stay, and it is reasonable to conclude that consumer demand for more efficient, high-powered and ultra-sophisticated "personal digital assistants" (PDAs) will only increase.[20] It is quite staggering what these PDAs can do—including touch screen capabilities, wireless connectivity, synchronization with other devices, automobile navigation, medical and scientific uses, educational uses, sporting and entertainment uses, and enhancements for people with disabilities.[21]

There are significant implications for these new technologies concerning the employer/employee relationship. Specifically:

> [t]he evolution of technology and the growth of business appear to go hand-in-hand. Tools of the trade 20 years ago included a day planner, desktop computer, fax machine, and telephone. There was a clear division between tools a company purchased for its employees and those professionals purchased personally.[22]

Put another way, the use of Blackberrys "is so convenient that it becomes part of one's daily routine, *blurring the line between business and personal device in the mind of the user*."[23] How, then, are employers to handle issues related to converging technologies, such as PDAs? In the Supreme Court's tangled Fourth Amendment jurisprudence, will employees have a subjective expectation of privacy that the public would find

---

[19] *Id*. at 357.

[20] *See* Alison Johnson, *Demand Factors*, TRADERS, Apr. 26, 2001, http://www.business.uiuc.edu/leuthold/econ102/WebProjects/Traders/section2.htm (arguing that demand for PDAs will continue to grow).

[21] *See* Craig Freudenrich & Carmen Carmack, How PDAs Work, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gadgets/travel/pda2.htm. *See also* Net Industries, Personal Digital Assistant (PDA), The Free Encyclopedia of eCommerce, Personal Digital Assitant (PDA), http://ecommerce.hostip.info/pages/851/Personal-Digital-Assistant-PDA.html (last visited Apr. 25, 2010).

[22] Kevin V. Maltby, *Employee Blackberry Use: What Is Private, and What Is Employer-accessible?*, BUS. WEST, Sept. 15, 2008, *available at* http://www.baconwilson.com/publication/pdf/323/9-15-08EmployeeBlackberryUse.pdf. This is one of the key concerns of our Article. We are interested in exploring the "blurring of the line" between what is personal and what is accessible to employers. This line is easily drawn with things like desktop computers, and even laptop computers to some degree because of their singular focus on the production of written materials or exchange of e-mails. But PDAs combine e-mails with text messaging, phone conversations, and internet access all in a 24/7 accessible device. This is precisely why they are so popular.

[23] *Id*. (emphasis added).

reasonable?[24]

Once we accept that these new technologies are here to stay, the questions then become a bit clearer: What limits do we place on the ability of employers (and the government?) to use technology to peek into our lives as employees and private citizens? What reasonable limitations can employers place on employees that will allow employers to prevent abuse of company time and equipment? What role do state and federal courts play in this process? What about state and federal agencies? And what issues do private citizens need to be aware of regarding these issues?

The outcome of these issues has major implications for judges and lawyers. For example:

> [i]n a . . . case in Canada involving allegations of breach of confidence by employees, BlackBerry e-mails and messages disseminated from the corporate owned Blackberry, including PIN messages sent between users using PIN identification, were used in evidence. There was some surprise not only that such evidence was admissible but that it was even available.[25]

III. COMPETING INTERESTS CUT ACROSS MANY TECHNOLOGIES

According to a recent study, some thirty-nine percent of Americans have "positive and improving attitudes" about their mobile communication devices, which in turn draw them further into engagement with digital resources.[26] Most American workers use the Internet or e-mail at work, more than half have

---

[24] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While this case was in the context of criminal procedure and whether a search has occurred under the Fourth Amendment, the analysis may still bear on questions of privacy in the workplace and what rights employers have to access employee information as it is related to PDA use.

[25] Bob McDowall, The Privacy of the BlackBerry: The Black Berry with the Bugs!, IT ANALYSIS, Jan. 31, 2005, http://www.it-analysis.com/content.php?cid=7718. McDowall writes:

> [T]here is a perception that when messages are sent using PIN to PIN protocol, they cannot be traced through logging or monitoring procedures by the BlackBerry Enterprise server. Clearly that is not the case. Indeed, in the current paranoid environment where corporate governance and listing regulations demand that all central, as well as external corporate communications are logged, archived and must be reasonably accessible, companies use software to log BlackBerry PIN communications.

Id.

[26] JOHN HORRIGAN, THE MOBILE DIFFERENCE 3 (Pew Internet & American Life Project Mar. 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/The_Mobile_Difference.pdf (emphasis omitted).

both personal and work e-mail accounts, and many say they check their personal e-mail from work on a daily basis.[27] Ninety-six percent of workers make use of e-messaging technologies in some manner, by accessing the Internet, using e-mail, or owning a wireless phone.[28] Most notably, seventy-three percent use all three technologies and nearly half report doing "at least some" work from home.[29] These trends result in a very broad community of Americans impacted by e-messaging policy, including both general usage and employer issues.

A. The Five Technologies:

Before moving forward, it will be useful to quickly lay out the various technologies that can be used for e-messaging. E-messaging encompasses many forms of communications technology. Increasingly, most Americans use a combination of these technologies for business and personal reasons, as part of their increasingly blended communications and lives.[30] Through technology convergence, these services are becoming more integrated and therefore less distinguishable. Like Hansel and Gretel dropping breadcrumbs as they walked through the enchanted forest, today, e-messaging users drop digital crumbs every time they utilize e-messaging services without knowing who may pick them up and why. In so-called "closed communities"[31] such as employers and some institutions, system

[27] MARY MADDEN & SYDNEY JONES, NETWORKED WORKERS iv (Pew Internet & American Life Project Sept. 24, 2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf.pdf.

[28] *Id.* at ii (describing the high percentage of workers who use one or more forms of e-messaging).

[29] *Id.* at i, iii (further describing e-messaging usage patterns among workers, and their use of e-messaging forms to work from home, further blending work and personal lives).

[30] *See id.* at iii, 29–34 ("73% of all workers use all three basic tools of the information age: they use the internet, have an email account, and have a cell phone.").

[31] The Internet has provided a powerful communications means for all kinds of institutions including commercial organizations (employers), academic entities, non-profits, and others. These organizations typically build their own internal networking environments, often called an "intranet," for internal communications that in turn connect to the Internet for external communications. These intranets are closed communities that generally require identification, authentication, and authorization to enter and use. To protect confidential information and minimize negative productivity impacts, these organizations often impose additional technical controls and usage policies on their user communities, acting as yet another service provider in the service provider chain. *See* The Data & Analysis Center for Software,

ownership issues also complicate policymaking, including whether end user devices are employer- or employee-owned and whether blended personal and business use is permitted. As shown in the attached diagrams, while the technical implementation of these five approaches significantly varies, the user-interaction flow is nearly identical.

1. Telephone (Voice) Systems

Telephone systems are often distinguished from other e-messaging forms because telephone conversations are aural, and conversation records are not generally stored on computer systems.[32] This distinction fades, however, upon recognition that there is no real technology barrier to creating such records. Rather, it is simply an artifact of the underlying technology and traditional policy and engineering choices.

While more recent e-messaging technologies create a computer-based record as an inherent part of the technical means, traditional telephone systems must be purposefully augmented to store message content.[33] As telephone systems have matured, however, enhanced services do use computer systems to transmit and, in some cases, store conversation records. For example, voice mail systems store spoken messages, and users can employ retrieve-and-reply functions to create a conversation.[34] Voice over Internet protocol (VoIP) systems provide telephone services over the Internet and use personal computer software that can buffer and store conversations, sometimes without the knowledge of all conversation participants.[35] Finally, telephone and Internet service providers now further blur traditional distinctions by

Intranets, http://www.thedacs.com/databases/url/key/178 (last visited Apr. 25, 2010); *see also* Bradley Mitchell, *Intranet*, ABOUT.COM, http://compnetworking.about.com/cs/intranets/g/bldef_intranet.htm (last visited Apr. 25, 2010).

[32] *See* FEDERAL COMMUNICATIONS COMMISSSION, FCC CONSUMER FACTS: RECORDING TELEPHONE CONVERSATIONS (Sept. 22, 2008), *available at* http://www.fcc.gov/cgb/consumerfacts/recordcalls.pdf.

[33] For example, consider the extensive technical implementation work required by telephone service providers to comply with the Communications Assistance to Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2006), such that Congress allocated funding for certain network upgrades.

[34] *See e.g.,* Tim Crosby, *How Voicemail Works*, HOWSTUFFWORKS, http://communication.howstuffworks.com/how-voicemail-works1.htm.

[35] *See e.g,.* Robert Valdes & David Roos, *How VoIP Works*, HOWSTUFFWORKS, http://communication.howstuffworks.com/ip-telephony.htm. S*ee also* Federal Communications Commission, Voice-Over-Internet-Protocol, http://www.fcc.gov/voip/ (last visited Apr. 25, 2010).

offering services, sometimes called "unified messaging," that integrate telephone features such as call logs, voice messaging, and calling features (e.g., caller ID) with more current e-messaging forms, including e-mail.[36]

2. E-Mail

E-mail systems use interconnected computer networks to store and forward messages from one computer user to another.[37] While e-mail systems may be self-contained within a closed community of users, the more common situation provides Internet-based message exchange.[38] End users compose an e-mail message, address it to one or more intended recipients, and request the message be sent.[39] Depending on the e-mail system used, messages may contain simple text, pictures, file attachments, or other content, including voice and video components. The message content is stored on a series of computers as it is transmitted to the recipients, according to Internet technical standards.[40] Thus, e-mail systems create message content records as an inherent part of the underlying technology, also known as "store-and-forward."[41]

[36] *See, e.g.,* Frequently Asked Questions About qHome Integrated Message Manager, About qHome, Integrated Message Manager, http://www.qwest.com/residential/products/qhome/qHome_FAQs.pdf; Verizon Wireless, Questions & Answers: What is the Verizon Hub?, http://support.vzw.com/faqs/Equipment/hub.html (last visited Apr. 25, 2010); Jefferson Graham, *Google Voice to Offer Free Calls, Centralized Number*, USA TODAY, Mar. 13, 2009, at 4B, *available at* http://www.usatoday.com/tech/products/2009-03-12-google-voice_N.htm.

[37] *See* V. ANTON SPRAUL, COMPUTER SCIENCE MADE SIMPLE 105 (Roger E. Masse ed., Broadway Books 2005); J. Edward Casteele, *How Does Email Work*?, EHOW, http://www.ehow.com/how-does_4815237_email-work.html; *see also* PC Mag.com, Definition of: Email, http://www.pcmag.com/encyclopedia_term/0,,t=&i=42233,00.asp (last visited Apr. 25, 2010).

[38] PHILIP E. MARGOLIS, RANDOM HOUSE WEBSTER'S COMPUTER & INTERNET DICTIONARY 190 (3rd ed. 1999).

[39] *See e.g.,* Learnthenet.com, Step-by-Step: Sending an E-mail Message, http://www.learnthenet.com/english/html/92email.htm (last visited Apr. 25, 2010).

[40] Internet-based e-mail works worldwide according to a set of technical standards and naming conventions set by various groups, including the Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), and the Internet Corporation for Assigned Names and Numbers (ICANN). *See* Int'l Eng'g Task Force, About the IETF, http://www.ietf.org/ about/ (last visited Apr. 25, 2010); International Organization for Standardization, About ISO, http://www.iso.org/iso/about.htm (last visited Apr. 25, 2010); Internet Corporation for Assigned Names and Numbers, About, http://www.icann.org/en/about/ (last visited Apr. 25, 2010).

[41] *See* PCMag.com, *supra* note 37; PCMag.com, Definition of: Store and

Closed communities, such as employers and institutions, further complicate the e-mail scenario. Many Americans use both personal and business e-mail addresses.[42] Business e-mail messages are typically created, sent, and received using employer-owned systems. Messages of a personal nature may be sent using the employer's system, or employees may choose to access personal e-mail accounts using webmail services and the employer's Internet connection.[43] In the webmail case, the message content is stored on the e-mail service provider's system, but monitoring technologies are available that may allow employers to access content when employees review their messages within the organization's environment.[44] Some closed communities choose to limit employee access to websites, including webmail services.[45]

3. Text Messaging

Text messaging evolved from paging technologies and, much like e-mail, allows the user to compose and send messages.[46] Unlike e-mail messages that often include graphics, file

Forward, http://www.pcmag.com/encyclopedia_term/0,,t=&i=52111,00.asp (last visited Apr. 25, 2010).

[42] MADDEN & JONES, *supra* note 27, at iv.

[43] Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 TOURO L. REV. 647, 656 (2007). Webmail services provide access to e-mail accounts using an Internet web browser. Employees may use these accounts on freely available services or as part of a personal customer relationship with an Internet service provider. *See, e.g.*, Gmail, http://www.gmail.com (last visited Apr. 25, 2010); Yahoo!, http://www.yahoo.com (last visited Apr. 25, 2010); Hotmail, http://www.hotmail.com (last visited Apr. 25, 2010).

[44] Sherman, *supra* note 43, at 661.

[45] There are a variety of vendors that provide web filtering software to allow closed communities to limit Internet usage. Organizations often cite security and productivity impacts as drivers for such usage limits along with concerns that users may create liability for the organization if they engage in illegal activities while using the closed community network, such as harassment or viewing child pornography. For a brief discussion of the issues that organizations must consider and drivers for implementing these controls *see* Jim Rendon, *Networking News: Balancing Web Filtering and Employee Privacy*, SEARCHNETWORKING.COM, Aug. 20, 2003, http://searchnetworking.techtarget.com/news/interview/0,289202,sid7_gci920223,00.html. *But see* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556, 559–62 (S.D.N.Y. 2008) (holding that employer acted improperly under Stored Communications Act by accessing employer's personal e-mails, which were stored and accessed directly from accounts maintained on outside service).

[46] Brian Gilmore, *Wireless Text Messaging*, CONNECTIONS MAG., Jan./Feb. 2004.

attachments, and other rich content, text messages are typically short phrases.[47] The technology limits of "texting" encourage users to employ abbreviated, often cryptic language.[48] Text messaging also employs a store-and-forward technology to transmit the message over the service provider's network to the recipient.[49] While the underlying technologies differ, the user experience for texting and instant messaging is very similar.

4. Instant Messaging (IM)

Instant messaging (IM) technologies developed to provide a real-time conversation experience for computer users in different locations. In an early case, the court noted, "[t]his communication is most like a telephone conversation,"[50] because the participants can interact with each other immediately. Recently, service providers have further blurred any distinction that existed between traditionally aural telephone calls and IM by adding "pc-to-voice" calls and "voice and video chat" features to IM services.[51] While the underlying technologies differ, much like texting, IM technology encourages the use of abbreviated language that may be difficult to decipher outside the conversation's context.

In closed communities IM raises many of the same issues as e-mail. Institutions may deploy IM services within their internal information technology (IT) infrastructures for business purposes, or employees may choose to access personal IM accounts on freely available services using the organization's Internet connection.[52] In yet another example of their

[47] Ancomm.com, What is Online Messaging?, http://www.ancomm.com/igeneration/what_is_online_messaging.html (last visited Apr. 25, 2010).

[48] David Allen Larson, *Technology Mediated Dispute Resolution (TMDR): A New Paradigm for ADR*, 21 OHIO ST. J. ON DISP. RESOL. 629, 633–34 (2006). Text messages may be sent using personal computers but, more often, users send messages from wireless phones with limited keypads. So, a texting language has evolved using various abbreviations and conventions, including those used to convey emotion. For example, "lol" is used for "laugh out loud," "cu2nite@8" for "see you at 8:00 pm," or given the technology's popularity among teenagers, "pos" for "parent over shoulder."

[49] Steve M. Nash, SMS: About SMS or Short Message Service…, TEXTMEFREE.COM, http://www.textmefree.com/sms.html.

[50] United States v. Maxwell, 45 M.J. 406, 411 (C.A.A.F. 1996).

[51] *See, e.g.*, Google Chat, http://www.google.com/talk/ (last visited Apr. 25, 2010) (describing capabilities for users to converse using voice, video, and traditional text for chat purposes).

[52] *See, e.g.,* Ahttp://www.aim.com (last visited Apr. 25, 2010); MSN, Messenger, http://www.msn.com/defaulta.aspx (last visited Apr. 25, 2010);

increasingly blended lives and communications, employees often use these freely available services for both business and personal purposes.[53] As with webmail, technologies are available that can block IM services or monitor and store IM content within closed communities.[54]

5. Social Networking Websites and Broadcast Messaging

Social networking websites, such as Facebook, MySpace, and LinkedIn, allow users to create a personal profile page and then interact with other site users to create communities of interest and mutual benefit.[55] The main purpose of these sites is to "act as a connector between users."[56] They frequently include their own messaging mechanisms that integrate with e-mail and other e-messaging forms, offering a rich, interactive environment and calling for a broader view in creating privacy standards.[57] Often cited as a key part of the Web 2.0 generation of Internet services, these sites are notable for the enormous amount of user-generated content they contain, including add-on applications, user groups, and other related functions that grow as the number of site users increase.[58] In some cases, users are even able to create their own social networking forum, based on a particular area of interest and open to their selected community.[59] Users

Google Chat, *supra* note 51.

[53] *See* Phillip M. Perry, *Chat Attack: Internet Messaging Can Be Costly for Employers*, 24 NO. 2 LEGAL MGMT. 32, 33 (2005); Matthew E. Swaya & Stacey R. Eisenstein, *Emerging Technology in the Workplace*, 21 LAB. LAW. 1, 5 (2005).

[54] *See Instant Messenger Security Securing Against the "Threat" of Instant Messengers*, http://www.technicalinfo.net/papers/IMSecurity.html (last visited Apr. 25, 2010).

[55] *See, e.g.,* Facebook, http://www.facebook.com (last visited Apr. 25, 2010). This site was originally created as an online mechanism for college students to connect but has grown to be used by a more generalized population. *See also* MySpace, http://www.myspace.com (last visited Apr. 25, 2010).This site bills itself as a "place for friends" and provides features to share music and other content in addition to messaging. *See also* LinkedIn, http://www.linkedin.com (last visited Apr. 25, 2010). This social networking service is designed for business professionals to facilitate networking and professional development along with recruiting and job searches.

[56] Patricia S. Abril et al., *Famous for Fifteen Minutes: IP and Internet Social Networking*, 6 NW. J. TECH. & INTELL. PROP. 355, 357 (2008).

[57] Daniel Findlay, *Recent Development: Tag! Now You're Really "It" What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C. J.L. & TECH 171, 175 (2008).

[58] *Id.* at 180.

[59] *See, e.g.,* Ning.com, Discover New Ning Networks, www.ning.com/discover (last visited Apr. 25, 2010) (describing how Ning allows the user to generate an

are also typically able to interact with their profiles and generate content from mobile devices, further blurring the distinction between social networking sites and other e-messaging forms.

More recent entrants to the e-messaging landscape, broadcast messaging services such as Twitter and Yammer, a Twitter-like service designed for use by closed communities, allow individuals to send short text messages to potentially large groups of "followers" at once.[60] Users send messages through the service provider's web portal that in turn distributes the messages to subscribers through various mechanisms including e-mail and text messaging.[61] These services provide users with the ability to connect and share personal information with others, much like social networking websites, but with short burst messages in real-time, sometimes called "microblogging."[62]

B. Summary of the Five Technologies

The distinctions between e-messaging technologies continue to blur as these technologies converge; providing a seamless user experience but exposing the fragmented nature of current policies. This trend is most evident in mobile communications where a single, consumer-class device now commonly provides telephone, e-mail, text messaging, IM, and web browsing

entire social networking site including messaging mechanisms targeted to a "community" in whatever manner the user defines it to be); *see also* Ning for Nonprofits: How to Create, Manage and Grow Your Social Network, http://www.casefoundation.org/blog/ning-nonprofits-how-create-manage-and-grow-your-own-social-network (Nov. 30, 2009).

[60] *Compare* Twitter, About, http://twitter.com/about (last visited Apr. 25, 2010), *and* Crystal, *What is Following?*, TWITTER, Nov. 6, 2008, http://help.twitter.com/entries/14019-what-is-following, *and* TwitterWedgie, www.twitterwedgie.com (last visited Apr. 25, 2010) (describing the service as follows: "[w]hat is Twitter? Twitter is a service for friends, family, and coworkers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?"), *with* Yammer, About Us, www.yammer.com/company (last visited Apr. 25, 2010), *and* Welcome to Yammer, http://blog.yammer.com/blog/press-1/ (Sept. 8, 2008, 13:14 EST) ("Yammer is a tool for making companies and organizations more productive through the exchange of short frequent answers to one simple question: 'What are you working on?'").

[61] Crystal, *How To Find Your Twitter Short/Long Code*, TWITTER, Nov. 11, 2008, http://help.twitter.com/forums/59008/entries/14226; Eddie, *I'm Not Receiving Emails from Twitter*, TWITTER, Feb. 2, http://help.twitter.com/entries/106799-i-m-not-receiving-emails-from-twitter.

[62] Twitter, Here There! Microblogging is Using Twitter, http://twitter.com/microblogging (last visited Apr. 25, 2010).

services.[63] Imagine asking the individuals who use these devices to calibrate their privacy expectations based on whether a specific conversation uses voice, e-mail, texting, IM, or web-based services such as social networking or broadcast messaging sites. Within closed communities, the issues are even more complex as employees utilize these devices to improve productivity, stay in touch with customers, and to provide 7x24 "on call" support in addition to supporting their personal communications needs.

The trend towards using mobile devices, especially in professional ranks, is further complicated by device ownership issues.[64] If the employer owns the device, then it can reasonably be assumed to be a part of the employer's computer systems. But what if an employee uses her own device to access her employer's systems? Does her expectation of privacy change if she is reimbursed by her employer for the e-messaging services that she uses to meet her work obligations? What if employer policies address personal device usage? What if they do not? These technology convergence and device ownership issues create a series of competing interests, and call for a more integrated view of e-messaging by all cultural stakeholders including the law. Moreover, these issues only grow thornier as Americans' online communications increase, and the lines between home and the workplace continue to blur.

C. Competing Interests

1. Users

Users expect privacy and support for managing their work-life balance as they utilize e-messaging services. As e-messaging technologies and cultural norms evolve, so will society's notion of what constitutes a reasonable expectation of privacy regarding them.[65] Moreover, as technologies converge and the distinctions among various e-messaging forms blur, users are less likely to distinguish between those forms. Individuals are more likely to

---

[63] *See, e.g.*, Verizon Wireless, Individual Plans, http://www.verizonwireless.com/b2c/splash/plansingleline.jsp?lid=//global//plans//individual (last visited Apr. 25, 2010) (description of Verizon Wireless 3G network services and devices).

[64] MADDEN & JONES, *supra* note 27, at viii ("professionals and executives own more gadgets").

[65] *See* Daniel J. Solove, *Do Social Networks Bring the End of Privacy?*, SCI. AM., Sep. 2008, *available at* http://www.sciam.com/article.cfm?id=do-social-networks-bring.

take a functional view. A user bases her expectation of privacy on how she uses the technology, such as to carry on a conversation, rather than on the specific technical means used. This functional view by users lends credence to the idea that society should—and likely will—recognize a reasonable expectation of privacy for e-messaging.

Newer forms of e-messaging—such as broadcast messaging services and social networking sites—further engage users and encourage them to share increasing amounts of personal information. According to one study, the share of adult Internet users who have a profile on at least one social networking site has more than quadrupled in the past four years.[66] Given the level of personal information shared in these e-messaging environments, users are particularly sensitive to changes in privacy policies, to the point that service providers may even back down from changes they plan for commercial purposes.[67]

Given this landscape, professionals are expected to carry mobile e-messaging devices and respond to work-related messages, with many saying that using these gadgets has resulted in demands that they work more hours.[68] These "tethered"[69] employees reasonably expect to use these devices for personal purposes. And using these technologies blurs "traditional lines between 'work' and 'home.'"[70] Many employees conduct business using personally owned devices or personal e-mail accounts, especially where they view their employer's policies regarding file transfers or remote access to the employer's computer systems as cumbersome or a barrier to getting their job done.[71] The blending of personal and

[66] Memorandum from Amanda Lenhart, Senior Research Specialist,Pew Internet & American Life Project on Adults and Social Network Websites (Jan. 4, 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf.

[67] *See, e.g.,* Posting of Gina Rubel to The PR Lawyer, http://www.theprlawyer.com/2009/02/facebook-nation-whats-in-their-privacy.html (Feb. 18, 2009. 6:13 EST). Facebook's attempted to change its privacy policy to allow it longer term retention and control over user-created content, and its quick about-face in light of negative publicity and user complaints. *Id.*

[68] MADDEN & JONES, *supra* note 27, at iv.

[69] *Id.*

[70] TRACY KENNEDY ET AL., NETWORKED FAMILIES 7 (Pew Internet & American Life Project 2008), *available at* http://www.pewinternet.org/Reports/2008/Networked-Families.aspx?r=1.

[71] *See* Joan Goodchild, *3 Reasons Why Employees Don't Follow Security Rules*, CSO, Oct. 29, 2008, http://www.csoonline.com/article/457575/3_Reasons_Why_Employees_Don_t_Follow_Security_Rules.

professional lives regarding e-messaging becomes even more profound when one considers the common practice of employers searching social networking and other sites for information on current and prospective employees.[72]

2. Service Providers

With traditional e-messaging services—such as telephones and even e-mail and text messaging—the concept of a "service provider" was quite clear. End users subscribed to a service, agreed to set terms of usage, and paid a fee for the service. Today's concept of "service provider" is more varied, and while Internet service providers (ISPs) still typically operate under the traditional model, broadcast messaging services, social networking sites, and other providers earn revenue via advertisements on their sites.[73]

Service providers want (and need) to make a profit, which is often based on the number of site visitors or advertisements displayed.[74] This means gathering and using potentially private information about their users to solicit certain advertisers. This approach requires the service provider to access and analyze the user's content, thus invoking concerns of confidentiality and data protection.[75] Various technology schemes, such as P3P (Platform for Privacy Preferences), have been developed in an effort to raise consciousness among users regarding the ways service providers handle the data they collect, but these technologies require user interaction and a detailed understanding to be effective.[76]

---

[72] *See, e.g.,* Robert Sprague, *Googling Job Applicants: Incorporating Personal Information into Hiring Decisions*, 23 LAB. LAW. 19, 37–38 (2007).

[73] *See generally* Louise Story, *How Many Site Hits? Depends Who's Counting,* N.Y. TIMES, Oct. 22, 2007, *available at* http://www.nytimes.com/2007/10/22/technology/22click.html (indicating there to be an increasing profitability of online advertising).

[74] For instance, consider Google's business model and advertising activities as described at Google, Corporate Information: Company Overview, http://www.google.com/intl/en/corporate/ (last visited Apr. 25, 2010); Google, Google Advertising Programs, http://www.google.com/intl/en_us/ads/ads_3.html (last visited Apr. 25, 2010).

[75] *See* Posting of Robert J. Driscoll et al. to Privacy & Security Law Blog, http://www.privsecblog.com/2009/07/articles/main-topics/marketing-consumer-privacy/advertising-industry-publishes-selfregulatory-principles-for-online-behavioral-data-collection/ (July 9, 2009) (discussing the advertising industry's initiative to curb privacy issues from abusing collection and analysis of user provided information online).

[76] See technical information on W3C, Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P (last visited Apr. 25, 2010). For a discussion on

3. Society

As with many good things, these new technologies are often used fraudulently.[77] Consequently, society has an interest in how e-messaging mechanisms are used. Law enforcement agencies may seek court-ordered access to service provider records and user-generated data within the boundaries of due process.[78] However, depending on the e-messaging service used (whether text, e-mail, or voice), user-generated content may not be preserved in many cases until *after* a court order is issued.[79] That is, many service providers do not preserve data unless ordered to do so; therefore, prior data may not be available. Law enforcement agencies have called for more extensive service provider data retention requirements in an effort to identify and prosecute criminals.[80]

Other countries, especially those in Europe,[81] have addressed this issue by mandating Internet service providers (ISPs) retain records of all user-generated traffic for extended periods of time that may then be accessed by law enforcement and other

the intense user engagement requirements and problematic nature of P3P, *see* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 754–55 (2000).

[77] Consider the persistence of e-mail-based fraud, sometimes called phishing, as described by the United States Computer Emergency Readiness Team. United States Computer Emergency Readiness Team, Report Phishing, http://www.us-cert.gov/nav/report_phishing.html (last visited Apr. 25, 2010). Consider also reports on the role Twitter played during the attacks on Mumbai in November 2008, such as CNN's report by Stephanie Busari, *Tweeting the Terror: How Social Media Reacted to Mumbai,* CNN, Nov. 28, 2008*,* http://edition.cnn.com/2008/WORLD/asiapcf/11/27/mumbai.twitter/.

[78] 18 U.S.C. §§ 2510–2513, 2515–2522 (2002).

[79] *See* Deborah H. Juhnke & David P. Stenhouse, *Technolawyer.com: Instant Messaging – What You Can't See Can Hurt You (in Court)*, 67 TEX. B.J. 518, 518–19 (2004); *see, e.g.*, Nicole Cohen, Note, *Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication*, 32 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 313, 319–20 (2006).

[80] *See, e.g.,* Declan McCullagh, *DOJ, Net Firms Fail to Agree on Data Retention*, CNET NEWS, June 2, 2006, http://news.cnet.com/DOJ,-Net-firms-fail-to-agree-on-data-retention/2100-1028_3-6079585.html (citing to a discussion between government officials and internet providers in reference to service providers recording data on their users).

[81] *See generally* CDT.org, Chapter Three: Existing Privacy Protections, Oct. 22, 2009, http://www.cdt.org/privacy/guide/protect (stating that the European Union had adopted a directive in regards to privacy and security for electronic communications).

government agencies.[82] In some cases, though, service providers have purposefully erased data to protect their users' privacy.[83] As e-messaging technologies grow, the tension between user privacy and surveillance as a means of protecting society will also grow. Some nations are looking to treat social networking traffic in the same manner as other e-messaging means.[84] Notably, at the same time, some members of the European Parliament are pushing for an effort "to define global standards for data protection, security and freedom of expression."[85]

D. Employers and Other Closed-Community Service Providers

Closed-community providers, most notably employers, also want to leverage e-messaging capabilities, while minimizing risks.[86] These organizations often provide a user's primary means of accessing the Internet, but under the control of school or workplace usage policies. Further, to remain competitive, employers need to attract and retain millennial generation talent who are entering the workforce as "digital natives,"[87] with strong skills and expectations around e-messaging. Thus, closed-community provider interests fall into three categories: (1)

[82] *See, e.g.,* BBC NEWS, *Net Firms Start Storing User Data*, Apr. 6, 2009, http://news.bbc.co.uk/2/hi/technology/7985339.stm.

[83] Mats Lewan, *Swedish ISPs to Erase Users' Data in Privacy Bid*, ZDNET, Apr. 29, 2009, http://news.zdnet.co.uk/internet/0,1000000097,39646148,00.htm.

[84] Greer McDonald, *Big Brother Watching Our Lives Online*, DOMINION POST, Apr. 4, 2009, *available at* http://www.stuff.co.nz/dominion-post/news/features/2313111/Big-Brother-watching-our-lives-online.

[85] Paul Meller, *Europeans Push for More Online Rights To Privacy*, MACWORLD, Mar. 6, 2009, http://www.macworld.com/article/139244/privacy.html.

[86] While employers are most often cited as service providers in the closed community settings, increasingly, other institutions such as schools and universities are employing similar controls to Internet usage as a means of decreasing the risk of data breaches, intrusions, and malicious software infections. In those settings, the use of such controls may be in tension with concepts of academic openness. Government agencies also face difficulties in managing their intranets, while balancing employee privacy interests. *See, e.g.,* Letter from Ari M. Schwartz, Information Security and Privacy Advisory Board, National Institute of Standards and Technology (NIST), to Jim Nussle, Director, The Office of Management and Budget (OMB) (Dec. 10, 2008) *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ISPAB_Einstein-letter.pdf (offering recommendations regarding the Einstein program).

[87] *See* Lee Rainie, *Digital 'Natives' Invade the Workplace*, PEW RES. CENTER PUBLICATIONS, Sept. 28, 2006, http://pewresearch.org/pubs/70/digital-natives-invade-the-workplace.

productivity and liability impacts, (2) the need to secure the organization's assets, and (3) risks to morale and retention.

E-messaging has provided real improvements in efficiency by automating routine approvals and correspondence, providing near real-time communications among team members, and supporting employee self-service functions to manage benefits and handle other common tasks.[88] A majority of workers say these technologies have improved their ability to do their jobs.[89] While these efficiency improvements motivate employers to utilize the technology, problems can easily arise. For example, "WITH JUST [sic] a few clicks of a mouse, an employer may lose valuable trade secrets and confidential information, be liable for violating copyright laws, or be exposed to claims that it permitted a hostile work environment."[90] Employee productivity may be hampered when other online activities simply "capture workers' attention at the office."[91]

To manage these risks, closed-community providers frequently monitor e-messaging, and a significant percentage of employers report having fired employees for telephone, e-mail, and other e-messaging misuse.[92] When an employer is on notice of abusive activity, failure to exercise reasonable care and report or take effective action to stop the abuse can have serious consequences. In *Doe v. XYC Corp.*, the Court held that once it was on notice, the employer had a duty to investigate an employee's alleged access to child pornography and "take prompt and effective action to stop the unauthorized activity . . . . No privacy interest of the employee stands in the way of this duty on the part of the employer."[93]

The *Doe* Court did not conclude, however, that employers have an affirmative duty to monitor employee activities in the absence of notice.[94] Thus, while employers may not be required to monitor employee activities, they must be prepared to act when

[88] MADDEN & JONES, *supra* note 27, at 3, 5–6, 8.

[89] *Id*. at 6.

[90] William G. Porter II & Michael C. Griffaton, *Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace*, 70 DEF. COUNS. J. 65, 65 (2003).

[91] MADDEN & JONES, *supra* note 27, at 10–11.

[92] Press Release, American Management Association, 2007 Electronic Monitoring & Surveillance Survey (Feb. 28, 2008), *available at* http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/.

[93] Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005).

[94] *See id*. at 1158, 1161–62.

given notice of abusive activities, including investigating and monitoring employee e-messaging activities, to avoid undue risk.[95] This situation may lead employers to increase their proactive monitoring in an effort to detect and react more quickly to abuse.

Also, closed-community providers—including employers and institutions such as universities—must protect their assets and are thus concerned with security risks created by e-messaging, including confidential data leakage, malicious software, and records management issues.[96] Confidential data takes many forms and incurs a wide range of risks, including data breaches that can lead to employee or customer identity theft, disclosure of trade secrets, or loss of competitive advantage. While such data leakage may be intentional, many situations are unintentional and result from a lack of user awareness or attention.[97] Further, organizations are obligated to protect certain data under both federal and state laws, especially in the case of financial, medical, or personally identifiable information.[98] By monitoring e-messaging, closed-community providers can identify specific patterns that suggest data leakage or malicious code infection (e.g., virus, Trojan code) and take protective action. Moreover, these organizations must also be prepared to locate and produce e-messaging records when there is a reasonable expectation of litigation, according to recent changes in the Federal Rules of Civil Procedure.[99]

Finally, in the employer setting, closed-community service provider interests in e-messaging privacy intersect with user (employee) interests where risks to morale and retention are

[95] *See id*. at 1158.

[96] *See, e.g*., ITS.SYR.edu, Stopping Data Leakage Starts with You, http://its.syr.edu/security/dataleakage.cfm (last visited Apr. 25, 2010) (noting Syracuse University's steps to provide their employees and students with a system that will help protect against data leakage).

[97] DAVID MEIZLIK, THE ROI OF DATA LOSS PREVENTION 3 (Websense 2008), *available* at http://www.websense.com/assets/white-papers/ROI_DLP_WP.pdf (citing PONEMON INSTITUTE, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH, (Nov 2007), *available at* http://www.encryptionreports.com/download/Ponemon_COB-2007_US_071127_F.pdf.

[98] *See, e.g.,* Katherine L. Kettler & John F. Hyland, *Privacy and Security in the Workplace: Employees as the Problem and Victim*, 93 PRAC. L. INST. PATENTS, COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES 227, 240–42 (2008) (noting the passage of numerous state laws mandating organizations to take reasonable measures of protection).

[99] *See* Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001); 105 AM. JUR. TRIALS § 22 (2009) [hereinafter AM. JUR. TRIALS].

concerned. The U.S. Supreme Court has stated that an employee's expectation of privacy must be an expectation that society is "prepared to consider reasonable.'"[100] Restrictive policies, including extensive monitoring, create undue stress and can lower morale and impair productivity.[101] Thus, since it is in their best interests, employers are motivated to balance their monitoring privileges with "employee quality of life."[102] Moreover, the millennial generation of employees now entering the workforce has grown up using a variety of e-messaging services and is accustomed to dispersing their attention across multiple, simultaneous tasks. They expect to use the same hardware and software at work that they use in their personal lives.[103]

On the surface, these competing interests among users, service providers, society, and closed-community service providers regarding e-messaging privacy may appear irreconcilable. However, ultimately all parties seek the same ends of balancing information access with protection, driving personal productivity, and minimizing risk. Therefore, balance is both desirable and achievable.

IV. FURTHER CONSIDERATIONS

E-messaging continues to evolve, with converging technologies now making a wide variety of services accessible from a single, often mobile, device.[104] Simultaneously, malicious software, unsolicited e-mails (sometimes called "SPAM"), and other security threats pose a constant risk to user and service provider assets.[105] Moreover, Web 2.0 and cloud computing trends are

[100] O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

[101] *See* Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-Mail Privacy*, 1 J. HIGH TECH. L. 101, 101, 106 (2002) (discussing the negative physical and emotional effects of workplace monitoring).

[102] Christopher Pearson Fazekas, *1984 Is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15, ¶ 3 (2004).

[103] Deborah Gilburg, *Management Techniques for Bringing Out the Best in Generation Y*, CIO, Oct. 26, 2007, http://www.cio.com/article/149053/Management_Techniques_for_Bringing_Out_the_Best_in_Generation_Y.

[104] *See*, *e.g.*, Verizon Wireless, Terms and Conditions, http://support.vzw.com/terms/products/ (follow "VZ Email" and "Unlimited Mobile to Mobile Messaging Bundle" hyperlinks) (last visited Apr. 25, 2010).

[105] Cisco.com, Cisco SCE 1000 Series Service Control Engine: Providing Service Security with Cisco Service Control Technology, http://www.cisco.com/

remaking the notion of "service provider" on the Internet, especially as improved data monitoring and collection technologies tempt these organizations to monetize user data streams with promises of added revenue opportunities.[106] Finally, within closed communities, business decisions to outsource e-messaging functions to managed services providers and use monitoring tools,[107] such as data leakage prevention, further complicate e-messaging policy questions. All these technology issues act as further confounders to achieving balance among competing e-messaging privacy interests, but technology can also act as an enabler, when used in a transparent and prudent manner.

A. Malicious Software, SPAM and Other Threats

The continued increase in computer security issues worries users and confounds service providers who wish to provide users with more e-messaging flexibility but also protect them from risks. High-profile attacks, such as those recently executed against the White House, both major-party 2008 presidential campaigns, Congressional offices, and one of the most infectious worms ever, serve notice that the threat is real.[108]

---

en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_brochure0900aecd8024ff1a.html (last visited Apr. 25, 2010); Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 299–300, 304 (2006); Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*, 9 INT'L J. COMM. L. & POL'Y 10 (2005).

106 Dion Hinchcliffe, *Why All The Fuss About Web 2.0?*, AIIM, Jan./Feb. 2010, http://www.aiim.org/infonomics/why-allthefuss-about-web2.0.aspx; Greg Lastowka, *User-Generated Content and Virtual Worlds*, 10 VAND. J. ENT. & TECH. L. 893, 901–02 (2008); *see*, *e.g.*, Matt Asay, *When Will Cloud Computing Start Raining Cash?*, CNET NEWS, Mar. 30, 2010, http://news.cnet.com/8301-13505_3-10471583-16.html (stating the profits companies have received from cloud computing).

107 *See*, *e.g.*, Kim Girard, *IBM Launches New Outsourcing Service*, CNET News, Dec. 9, 1998, http://news.cnet.com/IBM-launches-new-outsourcing-service/2100-1017_3-218910.html.

108 Posting of Derek Kravitz to Washington Post Investigations, http://voices.washingtonpost.com/washingtonpostinvestigations/2008/11/two_high-profile_incidents_of.html (Nov. 7, 2008, 18:48 EST); *see also* Shane Harris, *Hacking the Hill*, NAT'L J. MAG., Dec. 20, 2008, *available at* http://www.nationaljournal.com/njmagazine/cs_20081220_6787.php (stating that the Congressional Budget office and a Representative's office were hacked into). Also, Worms are a form of malicious software that can self-propagate and move on to new hosts on their own. The recent 'conficker' worm is considered one of the more virulent events. For details, see the Internet cooperative that self-organized to minimize the threat at Conficker Working Group Homepage, http://www.confickerworking

In closed service provider communities, e-messaging provides a potential means for malicious software to enter an organization, unbeknownst to the user. Increasingly, individuals are specifically targeted by attacks known as "spearphishing"[109] and "whaling."[110] Here, the attacker sends SPAM or an IM message to the potential victim containing a file attachment or web link that, when executed, infects the victim's computer with malicious code.[111] The malicious code then harvests confidential information and sends it to the attacker. In its recent *Internet Security Threat Report*, Symantec, a leading information security services provider, noted that seventy-eight percent of the malicious software threats to confidential information actually exported user data.[112] Closed community service providers, such as employers, must consider these threats when designing e-messaging policies and protective measures. For instance, an employer may be tempted to impose severe e-messaging restrictions in hopes of minimizing the risk, but these measures are likely to fail since employees are more than willing to circumvent policies they view as unrealistic or burdensome.[113]

group.org/wiki/ (last visited Apr. 25, 2010).

[109] "Phishing" is a term commonly used to describe fraudulent e-mail or IM messages that attempt to lure the victim into opening a file attachment, visiting a web link, or taking other action that allows malicious software to infect the victim's machine or exposes confidential information. Phishing originally focused on gathering personally-identifiable information from users that could be used to commit identity theft. *See generally* United States Computer Emergency Readiness Team, *supra* note 77. More recently, "spearphishing" has developed as a practice of highly targeted phishing where the attacker seeks information not just from any potential victim but designs his attack to target specific organizations or individuals for compromise, often to steal confidential information. *See generally* Press Release, iDefense Labs, Spearphishing & Whaling Attacks Reach Record Levels (June 7, 2008) (available online), *available at* http://labs.idefense.com/news/press/bbb/. [hereinafter iDefense Labs].

[110] "Whaling" is an even more targeted form of phishing where the attacker attempts to compromise an executive, government official, or other high-value target. *See* iDefense Labs, *supra* note 109.

[111] Corey Ciocchetti, *The Privacy Matrix*, 12 J. TECH. L. & POL'Y 245, 292 (2007).

[112] SYMANTEC, SYMANTEC GLOBAL INTERNET SECURITY THREAT REPORT: TRENDS FOR 2008 8 (vol. XIV 2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[113] *See, e.g.,* Tim Wilson, *Study: Routine Misbehavior by End Users Can Lead to Major Data Leaks*, DARKREADING, Sept. 30, 2008, http://www.darkreading.com/security/management/showArticle.jhtml?articleID=211201249 (discussing a recent study commissioned by Cisco Systems and conducted by market research firm, Insight Express that found many employees circumvent their employer's technology privacy rules in using their office computer).

These security risks are especially troubling for service providers who must balance the needs of all users in the shared Internet environment. Terms of usage agreements typically reserve a right for service providers to disconnect users who engage in hacking, send unsolicited e-mails, or other activities that may be deemed harmful or illegal.[114] Often though, users are not even aware that their computers have become infected with malicious software and need to be educated, not disconnected.[115]

B. Web 2.0, Cloud Computing, and Who (All) is the Service Provider Now?

In early forms of e-messaging, such as voice and e-mail, users knew their service providers—it was the entity that sent a bill and the domain name clearly visible at the end of e-mail addresses.[116] Now, with centralized cloud computing services and Web 2.0 sites that allow users to create content and add on applications that provide even more services, the definition of a "service provider" is expanding. Users still connect to the Internet through their Internet service provider (ISP), but now also share their information with search engines, social networking sites, broadcast messaging services, and cloud-based software for both personal and professional purposes—all web-based functions created and run by a "service provider."[117]

---

[114] *See, e.g.,* Windows Live Help, Microsoft Service Agreement Last Updated: March 2010, http://help.live.com/help.aspx?project=tou&mkt=en-us (last visited Apr. 25, 2010) (describing the user code of conduct and how customers may use the service).

[115] For example, a user's machine may become infected with malicious software, sometimes called a 'bot,' that takes over the PC and uses it to send spam, collect personal information, or launch denial of service and other attacks. *See generally*, United States Computer Emergency Readiness Team, FBI's "Operation Bot Roast II" Identifies and Captures Eight Individuals Responsible for Infecting Over 1 Million Comprised Computers, http://www.us-cert.gov/press_room/botroast_200711.html (last visited Apr. 25, 2010) (describing the FBI's recent success in identifying and capturing those responsible for infecting over one million computers). These malicious programs may be installed when a user visits a malicious website or executes a file attached from a malicious email. *Id.*

[116] *See* eNotes.com, Internet Regulation, http://www.enotes.com/everyday-law-encyclopedia/internet-regulation (last visited Apr. 25, 2010) (stating internet providers charge a fee for various services they provide, where subscribers connect to ISPs in numerous ways as well as provide consumers content including e-mail and video, as well as provide them with telephone numbers).

[117] *See id.*

Recently, some cloud-based services have garnered the attention of privacy advocates who have petitioned the FTC to investigate their security practices.[118]

These recently evolved Internet services provide even more power and flexibility to the user, but they can also leave a typical user puzzled as to where her data is stored, whose rules apply, and how to get assistance when her data is used in a manner that makes her uncomfortable.[119] Compounding matters even further, service provider terms of use and privacy policies vary widely even across seemingly similar services.[120] Most importantly, the boundaries across these services are increasingly blurred as users move through their personally-created spaces, calling for more consistency and standards of practice.

C. Service Provider Considerations

Technology improvements also impact the way service providers view the data created by their customers. While telephone carriers have always utilized network management and troubleshooting tools that may permit incidental call or data stream monitoring, improvements in Internet-based technologies now provide the means for service providers to monitor and

---

[118] *See, e.g.*, EPIC Complaint and Request for Injunction before the Federal Trade Commission, *In re* Google, Inc. & Cloud Computing Servs. (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf (stating Electronic Privacy Information Center's (EPIC) petition to the FTC requesting an investigation of Google's cloud computing services and data privacy practices); *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1186 (2009) (concluding that users are confused and do not recognize a variety of privacy issues, and often detailed computer controls can be worse for privacy, and is therefore drawing concern); Declan McCullagh, *Facebook Fights Virginia's Demand for User Data, Photos*, CNET NEWS, Sept. 14, 2009, http://news.cnet.com/8301-13578_3-10352587-38.html (noting a service provider resorting to ECPA and avoiding acting on a subpoena to gather user's personal information as part of worker's compensation action, as well as giving an example of current law applicability to Web 2.0 services and user protection from lawyers in civil cases seeking to mine data).

[119] *See generally* Yasamine Hashemi, Note, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 158 (2009) (explaining the intricacies of third-party applications on social networking sites and their various user terms and conditions).

[120] *See* ConsumerSearch.com, ISPs: Full Report, http://www.consumersearch.com/isp/cable-vs-dsl-and-satellite (last visited Apr. 25, 2010); Ron Miller, *Is Your ISP on Your Side?*, 8 SMART COMPUTING 103, Apr. 2002, *available at* http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/l0804/36l04/36l04.asp&guid=.

analyze user content in real-time.[121] These technologies can be used to enhance the user experience, for instance, by improving the network quality of service (QoS) for voice and video data streams that are highly sensitive to changes in network speed.[122]

From a privacy perspective, though, these same deep packet inspection (DPI) capabilities can be troubling if they are used to dissect and react to user traffic without the user's knowledge. These considerations became clear in the recent furor over behavioral-based advertising and resulting Congressional hearings.[123] At the same time, service providers seek alternative business models that allow them to offer low cost connectivity and cloud-based services at little or no cost to the user in return for directed advertising. Service providers must balance the revenue potential with user sensitivities, keeping in mind that many users do not fully understand the underlying technologies and their capabilities.

D. Special Considerations for Employers and Closed Communities

Closed communities, such as corporate and academic institutions, encounter additional challenges in today's evolving e-messaging environment, including privacy and legal implications that may be created by utilizing managed services.[124] Moreover, protective controls such as automated scanning, content monitoring, and data leakage prevention—in many ways, the closed community's version of deep packet inspection—help minimize the organization's exposure to malicious software and liability for inappropriate user activity

---

[121] *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1432.

[122] *See, e.g.*, CISCO SYSTEMS, INTERNETWORKING TECHNOLOGY HANDBOOK 49-1, *available at* http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.pdf (last visited Apr. 25, 2010) (discussing the technical purposes and implementation details of QoS to ensure better service for selected network traffic over various networking technologies).

[123] *See* Press Release, House Committee on Energy and Commerce, Energy and Commerce Committee Questions Data Practices of Network Operators (Aug. 1, 2008), *available at* http://energycommerce.house.gov/Press_110/110nr337.shtml (discussing the Committee's letter to ISP's and the resulting responses and hearings regarding deep packet inspection and behavioral advertising).

[124] *See* Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate*, WALL ST. J., Apr. 23, 2009, at A13, *available at* http://online.wsj.com/article/SB124045009224646091.html?mod=dist_smartbrief.

but can also create serious trust and morale issues for users.[125]

Increasingly, businesses and other closed community organizations will choose to outsource their e-messaging services, especially e-mail.[126] While using a managed services provider offers cost savings over maintaining in-house capabilities, given economies of scale, this approach further confounds e-messaging policy analysis. Current law permits an organization to access and monitor user e-mail on the employer's own e-mail servers.[127] If an organization outsources their e-mail services to another provider, will the employer or other institutional provider still be viewed as the "service provider," with the managed services provider acting as an agent, and so able to review user message content? Will the managed services provider be seen as a remote computing service (RCS), permitting access to the organization-subscriber?[128] On the other hand, might the e-messaging provider be viewed as an electronic communication service (ECS), limiting lawful access to the "intended recipient"?[129] Answers to these issues will have a profound effect on a closed community service provider's ability to monitor and investigate user activities.

While technology issues confound closed community service providers struggling with e-messaging policies, emerging technologies that improve automated message scanning may enable a more transparent, evenhanded approach to user monitoring. Using automated mechanisms, data leakage prevention tools focus on detecting and preventing confidential data loss events, such as employees using e-messaging to send employer-confidential information outside the organization.[130] These events may be intentional, such as an employee purposely

125 *See* Wesche, *supra* note 101 (discussing the employers' steps to protect themselves from improper employee computer use and negative physical and emotional effects of such workplace monitoring).

126 Press Release, Gartner Research, Gartner Says Enterprise E-Mail Hosting is Poised for Explosive Growth (Mar. 18, 2008), *available at* http://www.gartner.com/it/page.jsp?id=625809.

127 Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2004) (holding the employer to be the "service provider" under the exception provided by 18 U.S.C.A. § 2701(c)(1), entitling the employer to search messages on its servers).

128 18 U.S.C. § 2702(b)(3) (2010).

129 *Id*. at § 2702(b)(1).

130 *See* BARBARA FILKINS & DEB RADCLIFF, DATA LEAKAGE LANDSCAPE: WHERE DATA LEAKS AND HOW NEXT GENERATION TOOLS APPLY 8 (2008), *available at* http://www.sans.org/reading_room/analysts_program/DLL_April08.pdf.

removing customer information for fraudulent purposes; more often these are unintentional, such as asset mishandling or broken business processes that transmit unprotected confidential information over the Internet.[131]

Because these tools offer automated filtering mechanisms, closed community service providers, such as employers and academic institutions, can implement them in a manner that targets the information the organization needs to be concerned with and ignores a user's reasonable personal communications. Training programs can be used to explain the technology, its capabilities, and its usage to users. By sharing information on technical controls and methods, organizations can demonstrate their sensitivity to user privacy and assuage fears that others may be indiscriminately reviewing personal messages. Carefully implemented, this more balanced approach allows the closed community to protect its own environment from the risks of the open Internet while still maintaining the privacy and confidence of its users.

V. CURRENT LAW ON PRIVACY AND PROTECTION

The technical and functional distinctions between e-messaging technologies continue to blur, providing a seamless user experience but exposing the fragmentation in the law's current, technology-specific approach. A return to core privacy principles is needed. Early cases drew clear analogies between emerging e-messaging technologies and more traditional e-messaging forms, such as telephone calls.[132] In the meantime, though, courts have addressed these issues most frequently in employment situations and have favored employers over employees in reasonable expectation of privacy analyses, especially when the e-messaging activities fall into one of several very broad, technology-specific exception categories.[133] More recent cases show that courts may be willing to return to a privacy principle-based approach regarding personal e-mails and text messages.[134]

The current law regarding e-messaging privacy is further complicated by a wide variety of state-specific data protection

131 MEIZLIK, *supra* note 97, at 3.

132 United States v. Maxwell, 45 M.J. 406, 411 (C.A.A.F. 1996).

133 United States v. Long, 64 M.J. 57, 68–69 (C.A.A.F. 2006).

134 *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904–05 (9th Cir. 2008); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

and breach notification laws.[135] Moreover, the few court cases that have addressed social networking and other newer technologies have tended to focus on intellectual property and ownership issues.[136] Finally, recent changes in the Federal Rules of Civil Procedure have caused closed community service providers to retain and archive e-messaging data at a new level, compounding the potential for inadvertent exposure or breach of personal information.[137]

Unfortunately, this uncertainty in the law leaves e-messaging users and service providers without clear guidance, even in the current situation, let alone given the added complexity of converging e-messaging technologies and newer technologies such as social networking websites and broadcast messaging services.

A. Privacy & Protection

Congress established the Federal Communications Commission (FCC) with the Communications Act of 1934 and charged the Commission with "regulating interstate and international communications by radio, television, wire, satellite, and cable."[138] Thus, ISPs fall under the FCC's regulatory jurisdiction. The Internet has become a thriving virtual marketplace, and so the Federal Trade Commission's (FTC) charter to protect consumers and police anticompetitive practices plays an important role in regulating Internet, which includes e-messaging activities—especially as these technologies converge.[139] Current law limits accessing and monitoring

[135] As of December 9, 2009, forty-five states, the District of Columbia, Puerto Rico, and the Virgin Islands have all enacted some form of a security breach notification law. NCSL.org, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Apr. 25, 2010) [hereinafter State Security Breach Notification Laws].

[136] *See* Google, Inc. v. Affinity Engines, Inc., No. C 05-0598 JW, 2005 WL 2007888, at *1, 7 (N.D. Cal. Aug. 12, 2005).

[137] AM. JUR. TRIALS, *supra* note 99.

[138] *See* Federal Communications Commission, About the FCC, http://www.fcc.gov/aboutus.html (last visited Apr. 25, 2010). The FCC has recently taken enforcement actions against service providers who failed to file appropriate certifications regarding their practices to protect Customer Proprietary Network Information (CPNI). *See* Notice of Apparent Liability for Forfeiture before Federal Communications Committee, *In re* Annual CPNI Certification (Feb. 24, 2009), *available at* http://www.fcc.gov/eb/Orders/2009/DA-09-426A1.html (footnotes omitted) [hereinafter Notice of Apparent Liability].

[139] *See* Federal Trade Commission, About the Federal Trade Commission, http://www.ftc.gov/ftc/about.shtm (last visited Apr. 25, 2010). The FTC also

communications, including e-messaging, by service providers and others.[140] Newer e-messaging technologies such as social networking sites and other cloud-based services may also fall under various laws targeted to specific data collector types and state-specific laws regarding data protection and breach notification.[141]

Currently, the law treats different e-messaging technologies differently, and closed community service providers such as employers and other institutions complicate the situation further. Service providers have long been legally permitted, within reason, to monitor user content as incidental to managing and protecting their networks.[142] In the closed community scenario, courts have interpreted the federal wiretapping statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, later amended by the Electronic Communications Privacy Act (ECPA) of 1986,[143] as permitting employer monitoring of telephone calls but only under certain conditions.[144] Employers may monitor calls in the "ordinary course of business" where employees have been given notice of the practice, but employers must not listen to personal calls beyond the time necessary to determine the call's purpose.[145]

discusses a variety of enforcement actions taken against website operators under its authority to protect consumers from "unfair and deceptive [trade] practices," including regular news updates of current actions. *Id.*

140 18 U.S.C. §§ 2510–13, 2515–22.

141 Data protection laws have tended to focus on specific content types. *See, e.g.,* 15 U.S.C. § 1681 (2010) (noting that the Fair Credit Reporting Act focuses on consumer credit information); 47 U.S.C. § 521 (2010) (stating that the Cable Protection Act concerns itself with cable television records); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in 15 U.S.C. §§ 6801 *et seq.* (2006)) (stating that the act calls for protection of financial services data); *see also* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C) (stating that the act covers health and medical information); State Security Breach Notification Laws, *supra* note 135 (regarding the many states that have enacted some form of a security breach notification law).

142 *See, e.g.,* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–22 (2010)) (noting service provider exceptions).

143 18 U.S.C. §§ 2510–22.

144 *See* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 222–24, 227–31, 235–45, 248–49 (1994) (discussing courts' analyses of various federal statutes on employee privacy and forms of communication, particularly Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and its amendments).

145 *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 580, 582–85 (11th Cir.

Congress intended the ECPA to extend wiretapping protections to e-messaging technologies but introduced several more exceptions that have provided closed community service providers, such as employers, broad latitude in monitoring e-mail, instant messaging, and other e-messaging forms.[146] Most importantly, the ECPA includes a service provider exception that allows routine monitoring of electronic communications systems by the service provider for various purposes.[147] This exception also grants closed community service providers, such as employers, broad latitude in monitoring communications, and courts have frequently sided with them.[148]

The Stored Communication Act (SCA) further complicated the e-messaging privacy analysis by making a distinction between information in "transmission" and "storage."[149] Many e-messaging technologies utilize store-and-forward techniques that temporarily store messages during the transmission process.[150] Focusing on the technical details of e-mail, in *United States v. Councilman* the court held that, "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process."[151] Thus, messages in transit via store-and-forward techniques appear to have the same protections as "electronic communications" under the ECPA, but

1983) (describing limits on employer monitoring of employees' telephone calls and discussing a number of other cases with similar characteristics and holdings).

146 *See* 18 U.S.C. §§ 2510–22 (including provisions that brought technological advances such as e-mail and other forms of electronic communication under the scope of the statute); Greenberg, *supra* note 144, at 232–33.

147 18 U.S.C. § 2510 (5)(a)(ii).

148 *See* Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 114–15 (3d Cir. 2004) (holding that as a service provider, an employer could search e-mail messages on its systems); Bohach v. City of Reno, 932 F. Supp. 1232, 1233–35, 1236–37 (D. Nev. 1996) (describing the city as a service provider and thus entitled to review all messages from text paging system); Smyth v. Pillsbury Co., 914 F. Supp. 97, 98, 101 (E.D. Pa. 1996) (finding no reasonable expectation of privacy for employee e-mails on employer's system, despite repeated assurance from employer that messages were confidential); Kinesis Advertising, Inc. v. Hill, 652 S.E.2d 284, 296 (N.C. Ct. App. 2007) (stating employers entitled to access e-mail and voice mail messages as service provider); Greenberg, *supra* note 144, at 238–45.

149 18 U.S.C. § 2701–11 (2006).

150 *See* discussion *supra* Parts II.A—II.C (discussing the use of store-and-forward by e-messaging technologies such as e-mail, text messaging, and instant messaging); *see also* Memorandum from J. Klensin, Editor, AT&T Laboratories, Simple Mail Transfer Protocol (Apr. 2001), *available at* http://www.ietf.org/rfc/rfc2821.txt.

151 United States v. Councilman, 418 F.3d 67, 69–70, 79–80 (1st Cir. 2005).

the applicability of this analysis to newer e-messaging forms remains an open question.[152] The difficulty in demonstrating damages under the SCA was shown in a recent case where, despite the fact that an individual's e-messaging privacy was clearly and repeatedly breached, the court did not find that the statutory protections had been violated so as to compel the awarding of statutory damages.[153]

Despite the apparent latitude afforded employers, courts have recently held that employees "might" have a reasonable expectation of privacy for their e-mail messages based on the totality of circumstances.[154] This analysis, based on more traditional privacy principles, may herald a willingness to move away from the technology-specific approach and its myriad exceptions. As e-messaging technology continues to evolve and services converge, the technology-oriented approach is a dead-end. Reconsideration by the courts is a welcome sign.

The "key to legal [e-messaging] monitoring" by closed community service providers, such as employers, is providing "notice and [obtaining] consent."[155] Employers consistently win when they establish a formal, acceptable usage policy which provides employees with regular notices regarding monitoring.[156] Notices should be specific, understandable, and acknowledged by

[152] *See id.* at 79, 85 (holding that "electronic communication" includes transient electronic storage that is intrinsic to the communication process" and rejecting a proposed distinction between "in transit" and "in storage" for purposes of defining "electronic communication").

[153] Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 201, 206–10 (4th Cir. 2009) (finding that the plaintiff was not entitled to statutory damages, under the SCA absent a determination of actual damages).

[154] Kelleher v. City of Reading, No. CIV.A.01-3386, 2001 WL 1132401, at *5 (E.D. Pa. Sept. 24, 2001) (stating that plaintiff "might" have a reasonable expectation of privacy regarding her e-mail based on "the circumstances of the communication and the configuration of the e-mail system"); *see also* McLaren v. Microsoft Corp., No.05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *10–12 (Tex. App. May 28, 1999) (looking to the specific facts of the case to determine whether an employee had a reasonable expectation of privacy in the content of messages sent over his employer's e-mail system).

[155] Kettler & Hyland, *supra* note 98, at 237.

[156] *See* United States v. Simons, 206 F.3d 392, 395, 398 (4th Cir. 2000) (noting that an employee had no legitimate expectation of privacy in light of the employer's internet policy); United States v. Monroe, 52 M.J. 326, 328–30 (C.A.A.F. 2000) (holding there was no expectation of privacy on an e-mail system given notice that messages would be monitored); United States v. Rittweger, 258 F. Supp. 2d 345, 350–55 (S.D.N.Y. 2003) (finding that where the employee gave "express written consent" to monitoring and where notices were provided in the employee handbook he received, the employee had no reasonable expectation of privacy).

employees on a regular basis.[157] Employers must be careful, though, to ensure notices encompass all intended monitoring activities and that employees in positions of authority do not thwart the notices' effectiveness.[158] For example, in *United States v. Long* the court found that the notice focused on "maintenance and monitoring purposes" and held that the defendant had a reasonable expectation of privacy in the contents of her e-mail with respect to law enforcement searches.[159] Further, in *Quon v. Arch Wireless* the employer had a policy in place but a supervisory employee created an informal policy extension by repeatedly making statements that led employees to believe the contents of their text messages were private.[160]

Monitoring and access to user data and communications in more recent e-messaging forms is less clear. Social networking websites, broadcast messaging services, and other Web 2.0 capabilities are generally seen as akin to other, more clearly commercial websites.[161] The FTC governs their privacy policies and terms of usage under Congress's "broad prohibition against unfair and deceptive acts or practices."[162] As these e-messaging technologies converge, users are likely to find it increasingly difficult to discern among these different means of engaging in conversations and the current, disparate regulations. Finally, because these services often involve collecting and storing personally identifiable information, [163] they likely fall under the

157 Kettler & Hyland, *supra* note 98, at 229, 236, 239–40.

158 *Id.* at 229, 236, 239–45.

159 United States v. Long, 64 M.J. 57, 63–65 (C.A.A.F. 2006).

160 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906–07 (9th Cir. 2008) *cert. granted*, 77 U.S.L.W. 3619 (U.S. Dec. 14, 2009) (No. 08-1332).

161 *See* Federal Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Apr. 25, 2010) ("A key part of the Commission's privacy program is making sure companies keep the promises they make to consumers about privacy, including the precautions they take to secure consumers' personal information."); Electronic Privacy Information Center, In re Google Buzz, http://epic.org/privacy/ftc/googlebuzz/default.html (last visited Apr. 25, 2010) [hereinafter EPIC] (describing the urging of lawmakers for the FTC to investigate the privacy concerns of a social networking site clearly shows that such sites are viewed as within the FTC's grasp, just like clearly commercial sites).

162 *See* Federal Trade Commission, *supra* note 139 (discussing its broad powers delegated by Congress); Federal Trade Commission, *supra* note 161 (stating that the FTC has challenged numerous privacy policies under its authority to prohibit unfair and deceptive practices); *see, e.g.*, EPIC, *supra* note 161 (giving a specific example of how the FTC may use of its authority to investigate unfair and deceptive practices).

163 *See generally* ERIKA MCCALLISTER ET AL., NATIONAL INSTITUTE OF

scope of state-specific data protection and breach notification laws. Because these regulations vary from state-to-state,[164] users may be further confused as to their rights and protections when utilizing these newer e-messaging means.

B. A Quick Comment about Intellectual Property and E-Discovery Concerns

The few court cases that have addressed social networking and other Web 2.0 technologies have tended to focus on intellectual property and ownership issues.[165] For instance, Congress enacted the Digital Millennium Copyright Act (DMCA) in 1998 to protect copyright holders and limit service provider liability in the Internet age.[166] Copyright holders, such as music and recording companies, have sued social networking sites that provide communications mechanisms among users under the DMCA.[167]

While at least one of the more notable cases was voluntarily dismissed in April 2008, commentators have noted that social networking sites, with their user-created content and applications that facilitate uploading or sharing copyrighted material may call for courts to reconsider the current definition of "service provider" and "safe harbor."[168]

According to the Federal Rules of Civil Procedure, litigants must now provide for electronic discovery ("e-discovery").[169] This change creates a variety of challenges regarding social

STANDARDS AND TECHNOLOGY, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (recommending guidelines for protecting the confidentiality of personally identifiable information that is typically collected and stored by organizations).

[164] William E. Hartsfield, *Data Protection Laws*, 2 Investig. Employee Conduct § 13:19 (2010) (discussing the various privacy laws among the states).

[165] *See* Harris v. Lexjet Corp., No.A.3:09-CV-616, 2009 WL 4683699, at *1–3 (E.D. Va. Dec. 3, 2009) (focusing its analysis on copyright infringement laws); Facebook, Inc. v. Power Ventures, Inc., No. C 08-5780 JF (RS), 2009 WL 1299698, at *1–3 (N.D. Cal. May 11, 2009).

[166] Digital Millennium Copyright Act, Pub. L. No. 105-304, §§ 103, 202, 112 Stat. 2860 (1998). The DMCA provides a safe harbor for service providers who make a reasonable effort, when notified, to remove copyrighted material from offending sites. Digital Millennium Copyright Act § 512.

[167] *See* Hillel I. Parness, *Toward "Social Networking Law"?*, 1 NO. 4 LANDSLIDE 13, 14 (Mar./Apr. 2009) (discussing the lawsuit against MySpace for copyright infringement of musical works).

[168] *Id.* at 13–14.

[169] FED. R. CIV. P. 26(a)(1)(A), 26(b)(1)(B).

networking services.[170] Moreover, e-discovery requirements are especially pertinent to e-messaging privacy in the closed community case.[171] Employers can choose to use these requirements as a sword against employee privacy by recording, reviewing, and maintaining e-messaging content.[172] Two features of the e-discovery rules, however, may allow closed community service providers, such as employers, to use the rules as a shield to facilitate employee privacy and to protect themselves from extensive e-discovery costs.[173]

First, the amended Rule 26 incorporates a "two-tier" approach, allowing a party to avoid initially producing electronically stored information that is "not reasonably accessible because of undue burden or cost."[174] Second, Rule 37 now provides a safe harbor against sanctions for litigants who "fail[] to [produce] electronically stored information [that has been] lost as a result of the routine, good-faith operation of an electronic information system."[175] Courts can acknowledge, and even promote, user privacy by recognizing invasion of privacy as a cost factor that weighs against compelling production and calibrating their application of Rule 37's safe harbor to the level of e-messaging monitoring utilized within the closed community.[176] This approach could also be used to further protect user privacy by clarifying device ownership issues that arise when employees use devices they own to conduct business on behalf of their employer and limiting access to such data. As a result, the amended rules provide an opportunity to further user privacy interests from the bench, in those cases where closed community service providers, such as employers, have shown restraint against extensive monitoring practices.

---

170 *See generally* John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1203–04 (2007) (discussing the evolution of e-discovery requirements and the impact of social networking sites).

171 *See generally* Elaine Ki Jin Kim, *The New Electronic Discovery Rules: A Place for Employee Privacy?*, 115 YALE L.J. 1481, 1482, 1485 (2006) (suggesting how courts can shape e-discovery rules to protect privacy in the workplace).

172 *See id.* at 1482, 1485–86; Corey A Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces Vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, *1, 27 (describing legitimate methods for employers to monitor employees' use of company e-mail systems).

173 Kim, *supra* note 171 at 1486–88.

174 FED. R. CIV. P. 26(b)(2)(B).

175 FED. R. CIV. P. 37(e).

176 Kim, *supra* note 171, at 1488–89.

The bottom line is that courts are beginning to come full circle in their willingness to apply core privacy principles to e-messaging technologies, beyond just telephone calls. But uncertainty remains, especially with newer services such as social networking and broadcast messaging services. As e-messaging technologies continue to evolve and converge, users and service providers will face even more uncertainty, unless regulators, especially the FCC and FTC, step in now to lead with a consistent, technology-agnostic approach.

VI. ACHIEVING BALANCE

Despite competing interests, a balanced approach that serves all e-messaging stakeholder interests is achievable.[177] Regulators must look beyond past efforts that primarily addressed data collection and handling practices in amassing so-called digital "dossiers"[178] and instead look to today's new generation of user-created content and messaging. Further development in the law will be best achieved by joint rulemaking between the Federal Trade Commission (FTC) and Federal Communications Commission (FCC), consistent with their overlapping missions in the Internet age[179] and recognizing an expanded "service provider" definition. Most importantly, they must set identical policies in the areas of data privacy, protection, and property rights.

Many commentators have addressed individual issues or technologies, but few have connected the dots among the many e-messaging technologies now available, including the need to treat them in a similar manner, especially given the user's functional

[177] Daniel Solove lays out an excellent historical overview of data privacy laws. *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 1-1, 1-3, 1-27, 1-41–1-42 (Christopher wolf ed., 2006), *available at* http://ssrn.com/abstract=914271 (discussing the balance found in the Foreign Intelligence Surveillance Act).

[178] *See generally* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV 1393, 1394–95, 1398 (2001) (generally discussing the regulations of digital databases of information).

[179] *See supra* Part IV. There are other potential strategies that could be pursued. Options include either legislative reform that addresses e-messaging in a technology-agnostic manner while utilizing proven approaches to incentivize security innovation and best practices adoption, or evolution in e-discovery rules and practices to further ensure predictable, technology-agnostic treatment for user-created content. However, we are leaving the discussion in this article to the joint rulemaking prescription.

perspective that each of them simply supports a conversation.[180] At the same time, service providers must face technology challenges head-on by adopting best practices and acting in a transparent manner.[181] Finally, users must manage their e-messaging habits prudently and recognize their responsibilities as cyberspace makes a small world feel even smaller through our interconnections and online communities.[182] The burden of protecting online privacy should be shared by all these stakeholders.[183]

A. Legal Approaches

"[T]he Fourth Amendment protects people, not places."[184] In today's world of cyberspace communications, people must be identified with the various e-messaging communication mechanisms they use. As Warren and Brandeis pointed out in 1890, the right to privacy should not be limited to "any particular medium or form of expression."[185] Congress intended the ECPA to extend telephone privacy protections to other e-messaging forms,[186] but the lack of clarity and exceptions in that statute, along with varying interpretations by the courts, call for a return to basic principles.[187]

Recent cases have shown that courts are willing to use a principle-based approach in place of technology-based analysis. Reasoning in a manner similar to the approach used to limit wiretapping, the court in *United States v. Long* found that the defendant had a reasonable expectation of privacy for her workplace e-mail messages, since the notice provided referred

---

[180] *See generally* Wilson, *supra* note 170 (limiting its privacy and discovery analysis to social networking sites, such as Facebook and Myspace); Kim, *supra* note 171 (discussing only electronic surveillance technologies in the context of employee privacy).

[181] *See,* Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 87 (2007) (discussing measures internet service providers can take to manage privacy burdens).

[182] *Id.*

[183] *Id.*

[184] Katz v. United States, 389 U.S. 347, 351 (1967).

[185] Warren & Brandeis, *supra* note 1, at 205–06 (discussing recognition of a right of privacy).

[186] 18 U.S.C. §§ 2510–22.

[187] *See* Greenberg, *supra* note 144, at 231–32 (discussing the rationale for adopting the Electronic Communications Privacy Act of 1986).

only to "monitoring or maintenance" purposes.[188] Moreover, in *United States v. Forrester*, the Ninth Circuit recently held that the privacy interests in e-mail are "identical" to those in postal mail and that message contents in both may deserve Fourth Amendment protection.[189] Finally, just a few months ago, the court extended their *Forrester* view even further in *Quon v. Arch Wireless* to include text messaging and granted that, "[t]he recently minted standard of electronic communication via *e-mails, text messages, and other means* opens a new frontier in Fourth Amendment jurisprudence that has been little explored."[190]

Because the reach of e-messaging services "erases state and national borders,"[191] any legislative action to further address and clarify e-message privacy interests must be undertaken at a federal level to be effective. While an ECPA rewrite may be necessary to address e-messaging forms comprehensively, several incremental changes would be a positive step: redefining the scope to address e-messaging in a technology-agnostic manner; requiring notice for all monitoring activities; limiting, or even eliminating, the exception for communications service providers; and eliminating the now impractical distinction of transmission and "storage" activities, given the common use of store-and-forward technologies in e-messaging.[192]

A comprehensive legal approach to privacy and protection for e-messaging must also recognize the increasing overlap between the traditional regulatory missions of the FCC and FTC. In today's e-messaging environment that includes social networking sites, broadcast messaging services, and increasingly complex in-the-cloud applications and communications mechanisms, traditional separations between communications services and trade practices have blurred. Currently, these agencies each press their own agendas for data protection, reasonable privacy practices, and improved cyber security.[193] As e-messaging

188 United States v. Long, 64 M.J. 57, 64–65 (C.A.A.F. 2006).

189 United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

190 Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–05 (9th Cir. 2008) (emphasis added).

191 Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 293, 301 (2002).

192 *See* Greenberg, *supra* note 144, at 224–25, 249–52.

193 *See* Public Notice, Federal Communications Commission, FCC Seeks Nominations for Membership on the Communications, Security, Reliability, and

technologies converge, the time is ripe for these expert agencies to engage in a joint rulemaking process to provide consistent guidance and obligations for all e-messaging providers.[194] Users should not be asked to calibrate their privacy expectations on whether their messaging services are supported by a traditional communications carrier or an otherwise commercial website, nor should service providers be obligated to adhere to potentially conflicting guidance.

B. Service Provider Best Practices

Providing transparency in their practices around data collection, protection, and usage is the key action for service providers in creating a balanced information ecosystem. Recent regulatory actions have encouraged this kind of openness and

Interoperability Council (CSRIC) (Apr. 10, 2009), *available at* http://www.fcc.gov/Daily_Releases/Daily_Digest/2009/dd090410.html (describing the mission of the Communications, Security, Reliability, and Interoperability Council which includes "security, reliability, operability, and interoperability of public safety communications systems"); Federal Communications Commission, *supra* note 134 (explaining actions that are violations of the Communications Act); Federal Trade Commission, Fighting Fraud with the Red Flags Rule: Frequently Asked Questions, http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm#B (last visited Apr. 25, 2010) (describing the FTC's Red Flags Rule which requires businesses and organizations to implement a program "to detect the warning signs of identity theft in their day-to-day operations").

194 Recently the FCC and FTC have exhibited a willingness to collaborate in e-messaging related areas. FEDERAL TRADE COMMISSION, GN Docket No. 09-51, COMMENTS OF THE FEDERAL TRADE COMMISSION (2009), *available at* http://ftc.gov/os/2009/09/090904fccnbp.pdf ("The Federal Trade Commission, which shares jurisdiction over broadband Internet access and related content and applications with the Federal Communications Commission, appreciates this opportunity to contribute to the development of the Nation's Broadband Plan."). The FTC goes on to emphasize the need to protect consumer privacy and support data security. *Id.*; *see also* Wendy Davis, *FTC Urges FCC to Consider Behavioral Targeting in Broadband Plan*, MEDIA POST NEWS, Sept. 4, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=113057 (last visited Apr. 8, 2010) (stating that the FTC has brought internet privacy issues to the attention of the FCC); FEDERAL TRADE COMMISSION, *supra* note 191(urging the FCC to address behavioral advertising and other consumer privacy risks in its national broadband plan, especially with respect to packet inspection technologies). Also, the FTC has shown further willingness to collaborate with other agencies in areas of technology and consumer privacy. For instance, the recently promulgated FTC (FTC Breach Notification Rule) and Health and Human Services (HIPAA Breach Notification Rule) rules are aligned regarding personal health data breach notification, pursuant to the American Recovery and Reinvestment Act of 2009 (ARRA). *See* Health Breach Notification Rule, 74 Fed. Reg. 163 (Aug. 25, 2009) (to be codified at 16 C.F.R. pt. 318).

self-regulation.[195] Consumer participation in targeted marketing programs in more traditional retail settings show that many are comfortable with such data collection and use, if they know about it.[196] Service providers increasingly recognize the need for plain English, easy-to-use privacy policies, community vetting, and notice prior to changes.[197]

Service providers, including those in closed communities, should base their approach to balancing e-messaging privacy needs and risks on internationally-accepted best practices by utilizing widely accepted, standard privacy principles; developing clear e-messaging policies, where appropriate; adopting data minimization techniques, as is feasible; maintaining sound, current technical controls; and educating users on policy and e-messaging technologies.

First, service providers should seek guidance from standard widely accepted privacy principles. By adopting a well-respected approach, service providers save time by not reinventing the wheel, gain credibility with users, and demonstrate a reasonable level of diligence should the program be called into question at a later time (*e.g.*, litigation). One such resource from the internationally-recognized Organization for Economic Co-Operation and Development (OECD) focuses on eight principles for data collection, handling, and privacy assurance, including: (1) Collection Limitation, (2) Data Quality, (3) Purpose Specification, (4) Use Limitation, (5) Security Safeguards, (6) Openness, (7) Individual Participation, and (8) Accountability.[198]

---

195 *See, e.g.*, Federal Trade Commission, FTC Staff Revises Online Behavioral Advertising Principles, http://www.ftc.gov/opa/2009/02/behavad.shtm (last visited Apr. 25, 2010) (discussing the FTC's response to behavioral advertising).

196 Consider, for example, the popularity of grocery store discount cards where the consumer is given regular discounts in return for using a card at checkout time that allows the store to record and track purchases made. *See* Dawn Hawkins, Pros and Cons of Grocery Discount Cards, HELIUM, http://www.helium.com/items/1774018-pros-and-cons-of-grocery-discount-cards (explaining the reason stores provide grocery discount cards and the personal information collected from consumers).

197 *See, e.g.*, Google Privacy Center, http://www.google.com/intl/en/privacy.html (last visited Apr. 25, 2010) (containing plain English guidance on privacy policies and including instructive video clips).

198 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14–16 (2002); *see also* AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, INC. & CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, GENERALLY ACCEPTED PRIVACY PRINCIPLES 4, 7, 12–65 (2009), *available at* http://infotech.aicpa.org/NR/rdonlyres/0AB737BF-55D1-459B-ADD5-179A270E863C/

Essentially, service providers, and especially those in closed communities, can utilize principles from internationally-recognized organizations such as the OECD as a foundation, customizing their own e-messaging policies and practices according to their specific environment and needs.

For additional guidance on core privacy principles, the Federal Trade Commission has developed "five core principles of privacy protection" that include: "(1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress."[199] Additionally, the Federal Communications Commission (FCC) has declared that

> section 222 imposes the general duty on all telecommunications carriers to protect the confidentiality of their subscribers' proprietary information. The Commission has issued rules implementing section 222 of the Act. The Commission required carriers to establish and maintain a system designed to ensure that carriers adequately protected their subscribers' CPNI [Customer Proprietary Network Information]. Section 64.2009(e) is one such requirement.[200]

The FTC and FCC should jointly develop general privacy principles based on the historical OECD guidance, as well as the FTC and FCC current privacy mandates. These two organizations have independently addressed these issues. However, given the overlapping nature of today's e-messaging technologies in the workplace, these agencies must work together to produce identical privacy principles. And, these principles must not only be of an overarching nature, but also must be specific—and actionable—giving detailed requirements for each of the current communication technologies being used in the workplace and beyond. Finally, these specific details should be flexible enough to include new communication technologies as they emerge.

Second, closed community service providers, such as employers and academic institutions, should create a clear, formally

14378/GAPP_BUS_0909.pdf (stating that "generally accepted privacy principles" include: management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, and monitoring and enforcement).

[199] Federal Trade Commission, Report to Congress, http://www.ftc.gov/reports/privacy3/priv-23.shtm (last visited Apr. 25, 2010) ("This report to Congress provides an assessment of the effectiveness of self-regulation as a means of protecting consumer privacy on the World Wide Web.").

[200] Notice of Apparent Liability, *supra* note 138.

documented e-messaging policy as one component of a comprehensive governance, risk, and compliance (GRC) program.[201] "An effective [e-messaging policy] contains [several] key provisions."[202] The policy should define e-messaging and enumerate technologies such as telephone systems, e-mail, text messaging, and IM, but should also include broad language to account for technology changes and other services such as social networking and broadcast messaging services.[203] The policy should clearly state that all e-messaging systems and communications are the organization's property and are provided for the organization's mission or business purposes.[204] The policy must also provide users with notice regarding the organization's monitoring and access policy, and include statements regarding user consent, privacy expectations, and permitted personal uses.[205] Further, the policy should also explain that security controls such as passwords do not grant privacy rights.[206] Closed community providers often publicly post their policies regarding e-messaging and community member limits to further increase awareness of their approach.[207]

Next, all service providers should formally adopt data

[201] *See, e.g.*, SCOTT L. MITCHELL & CAROLE STERN SWITZER, ESQ., GRC CAPABILITY MODEL "RED BOOK" 2.0, Intro-viii, Intro-ix, Intro 24–25 (OPEN COMPLIANCE & ETHICS GROUP 2009), *available at* http://www.oceg.org/view/RB2 Project (describing a comprehensive governance, risk, and compliance framework).

[202] Jerome P. Coleman et al., *Electronic Communications and Privacy in the Workplace*, 762 PRACTISING L. INST., LITIG. & ADMIN. PRAC. COURSE HANDBOOK SERIES 597, 615 (2007).

[203] *See id.* at 614–17 (discussing the characteristics of an effective policy regarding monitoring of electronic communications such as e-mail, instant messages, and camera phone pictures).

[204] *Id.* at 615.

[205] *Id.*

[206] *Id.*

[207] *See, e.g.*, IBM, IBM Social Computing Guidelines, http://www.ibm.com/blogs/zz/en/guidelines.html (last visited Apr. 25, 2010) (outlining IBM's e-messaging policy with regard to blogs and other social networking sites designed to protect IBM bloggers and the company itself); Social Media – Telstra's 3 Rs of Social Media Engagement, http://www.nowwearetalking.com.au/library/pdf/news/social-media-company-policy_final_150409.pdf (last visited Apr. 25, 2010) (discussing the company's rules for employee participation in social media and online communities including the requirement of showing respect, representation, and responsibility for the company and communities in which the employer interacts); Oracle, Oracle Social Media Participation Policy, http://www.sun.com/communities/guidelines.jsp (last visited Apr. 25, 2010) (describing the company's social media participation policy as it applies to a wide array of online social activities occurring during work or outside of work).

minimization techniques when collecting information and managing e-messaging systems that may contain users' personal communications.[208] As described in typical e-messaging policies or usage agreements, service providers may access e-messaging systems for routine monitoring purposes (*e.g.*, to ensure customer service levels), to support litigation discovery or lawful requests, or as a part of investigative activities.[209] Data minimization techniques limit the information that the organization "acquires, retains, and disseminates" as part of these activities.[210] These techniques protect user privacy by collecting only information specifically needed for the present activity.[211] Moreover, by formally adopting and communicating their use of data minimization techniques, service providers gain credibility with users who may otherwise be concerned that their personal communications are being arbitrarily collected and retained.[212]

Further, by maintaining sound, current technical controls in their e-messaging environments, service providers protect both

---

[208] *See* David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 9:1 (2007) (describing the data minimization procedures required under the Foreign Intelligence Surveillance Act). Data minimization techniques have gained attention for their use in minimizing the personal information collected pursuant to certain forms of authorized surveillance); Ed Sutherland, InternetNews.com, Less Data, More Security (Jan. 17, 2007), http://www.internetnews.com/bus-news/article.php/3654211 (describing the growing trend and greater advantage of data minimization over retention of consumer information and stating that "information is a liability"). The basic concepts of balancing an individual's privacy interests with those of the investigating authority by limiting the data acquired, retained, and disseminated are also applicable in the employer-employee setting. *See id.* (discussing data minimization in the workplace context).

[209] *See* Coleman et al., *supra* note 202, at 614–17 (describing what an effective e-messaging policy entails); *see also* Privacy Rights Clearinghouse, Fact Sheet 7: Workplace Privacy and Employee Monitoring, http://www.privacyrights.org/fs/fs7-work.htm (last visited Apr. 25, 2010) (describing the ways in which employer's typically monitor of electronic messaging in the workplace).

[210] Kris & Wilson, *supra* note 208.

[211] *See* The New York Times Syndicate, *Data Minimisation May Plug Breaches*, EMIRATES BUS. 24/7 (Dubai), Apr. 5, 2009, *available at* http://www.business24-7.ae/opinion/analysis/data-minimisation-may-plug-breaches-2009-04-05-1.96445 (noting that data minimization techniques will allow companies to pinpoint only the specific date they need to keep a competitive advantage in the marketplace).

[212] *See* FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 3, 7, *available at* http://www.ftc.gov/infosecurity/ (providing businesses guidance in determining the amount and type of personal customer information to obtain and retain in order to maximize electronic security) [hereinafter PROTECTING PERSONAL INFORMATION].

their assets and user privacy.[213] Service providers may also be obligated under certain laws to protect personal information.[214] A sound information security program includes, among other things, maintenance of technical controls such as firewalls, anti-virus and anti-spyware software, password management, wireless and remote access protective measures, intrusion detection, and log maintenance.[215] Moreover, in closed communities, implementing emerging technical controls, such as data leakage prevention (DLP) software, also supports both organization and user interests.[216] These tools automate e-messaging content scanning and monitoring using advanced linguistics analysis.[217] E-messaging monitoring protects the organization, while using DLP tools that can be programmed to ignore personal communications minimizes the intrusion on user privacy.[218]

Finally, service providers should ensure users have appropriate training and information regarding e-messaging services, and, in the case of closed communities, management should partake in such training.[219] A recent survey showed that about eighty percent of employees use employer-issued personal computers for e-mail, and many of those employees are willing to tamper with security settings if they believe the settings are a hindrance.[220] A great deal of education is needed[221] and user training should include information not just about the rules but also the implications of user actions, such as the risk to assets

213 *Id.* at 9, 11, 13.

214 *See* Kettler & Hyland, *supra* note 98, at 240–42 (examining the personal information protection requirements under the Fair and Accurate Credit Transaction Act, the Fair Credit Reporting Act, and California consumer protection laws).

215 *See* Mary Brandel, CSO, Data Loss Prevention Dos and Don'ts, http://www.csoonline.com/article/221272/Data_Loss_Prevention_Dos_and_Don_ts (last visited Apr. 25, 2010); PROTECTING PERSONAL INFORMATION, *supra* note 212, at 9, 11, 13, 15–17.

216 *See* Brandel, *supra* note 215 ("[Organizations should] pilot DLP tools in [their] own environment[s] before deciding which ones will work best.").

217 *Id.*

218 *See* FILKINS & RADCLIFF, *supra* note 130, at 6 (discussing the use of access controls, encryption, increased VPN security, and filters for outbound personal information in order to avoid disclosing personal information).

219 *See id.* at 5, 9, 11; PROTECTING PERSONAL INFORMATION, *supra* note 212, at 17, 19; Kettler & Hyland, *supra* note 98, at 244–45.

220 Wilson, *supra* note 113 (citing a recent study commissioned by Cisco Systems and conducted by market research firm, Insight Express).

221 *Id.*

and privacy.[222] E-messaging service providers are uniquely positioned to protect their users' communications, and also engage those users in how they can best protect themselves, as seen in the cautions and tips sections now common to social networking sites.[223]

C. End User Rights, Responsibilities, and the Need for Common Sense

E-messaging technologies have increasingly "blurred [what were previously clear] lines between 'work' and 'home.'"[224] The conversational characteristics of many e-messaging forms, especially text messaging and instant messaging, encourage users to make offhand or rash remarks that, taken out of the moment, may be harmful or embarrassing to the user or, in the case of a closed community, an employer or institution. Practicing self-discipline and simply using common sense to stop and consider the potential impact of their communications—"think before you press send,"—is the best approach for users, whether acting in social networking communities, participating in closed communities, or simply using more traditional e-messaging services such as e-mail.

In addition, users must make a good faith effort to read, understand, and ask questions about service provider privacy and terms of use policies. Users serve themselves best by learning at least the basics of e-messaging technologies, including how messages are stored, managed, and monitored. Finally, closed community participants must also understand that using an organization's e-messaging systems may impact their privacy rights beyond the workplace. For example, employees may be waiving the attorney-client privilege when they communicate with their own counsel via their employer's e-mail system.[225]

---

[222] *See* Goodchild, *supra* note 71 (stating that employees should be educated to the dangers of accessing their personal information on public computers).

[223] *See, e.g.,* Facebook, Welcome to the Safety Center, http://www.facebook.com/safety (last visited Apr. 25, 2010) (providing links for specific safety queries, including a section for Parents, Educators, Law Enforcement Agencies, and Teens).

[224] KENNEDY ET AL., *supra* note 70, at iii, 26.

[225] Ruth E. Piller, Employees Cannot Expect Privacy in E-Mail Using Employers' Computers, LITIG. NEWS ONLINE, May 2008, http://www.abanet.org/litigation/litigationnews/2008/june/0608_article_email.html; *see, e.g.,* Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 438–41, 443 (N.Y. Sup. Ct.

VII. CONCLUSION

Service providers, users, and society need not be adversaries regarding e-messaging usage and privacy. Such a confrontational approach ultimately damages all stakeholders by limiting effective use of the most promising of our technological developments—improvements in working and communicating with one another. Nor must the Internet and e-messaging capabilities be viewed as a "privacy horror show."[226] Building a healthy, balanced information ecosystem that serves all stakeholder interests is achievable by recalling timeless privacy principles of self-determination while rethinking the current regulatory scheme.

Achieving this balance requires commitment from all stakeholders and calls for further development in the law, especially joint rulemaking by the FTC and FCC, given their overlapping missions in the Internet age. Contemporaneously, service provider transparency and best practices should be adopted along with user recognition of their rights and, more importantly, their responsibilities to act in a common sense and self-disciplined manner. Many commentators have addressed various technologies and portions of the e-messaging quandary, but the time is now ripe for the FCC and FTC to seize this unique moment in technology evolution and regulatory development to treat these technologies in a comprehensive manner. By broadening the definition of service provider to include all those who provide e-messaging services—wherever users engage in electronically-assisted conversations—and applying consistent privacy principles, based on internationally-accepted standards and practices, we can look forward to a time when an e-messaging user need not calibrate her expectation of privacy based on the specific technology or provider. "The law *can* protect privacy."[227]

2007).

[226] *But see* Schwartz, *supra* note 9 (describing the widespread disclosure of personal information over the internet as a "privacy horror show").

[227] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 228 (N.Y. Univ. Press 2004).