NO. 11-4847

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

PHILLIP A. HAMILTON,

Defendant-Appellant

On Appeal from the United States District Court
for the Eastern District of Virginia
at Richmond

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANT AND URGING REVERSAL

Marc Rotenberg
Counsel of Record
Alan Butler*
David Jacobs**
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

April 6, 2012

---

* Mr. Butler is currently admitted to practice in the state of California.
** Mr. Jacobs has satisfied the requirements to practice and is pending admission in the State of New York.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, 29(c), and Local Rule 26.1 *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock. No publicly held company has a direct financial interest in the outcome of this litigation by reason of a franchise, lease, other profit sharing agreement, insurance, or indemnity agreement.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1]

EPIC routinely participates as *amicus curiae* before the United States Supreme Court, federal circuit courts, and state appellate courts in cases concerning privacy issues, new technologies, and constitutional interests, such as: *FAA v. Cooper*, 132 S. Ct. ____, 2012 WL 1019969 (2012); *United States v. Jones*, 132 S. Ct. 945 (2012); *First Am. v. Edwards*, 610 F.3d 514 (9th Cir. 2010), *cert. granted* 131 S. Ct. 3022 (2011) (No. 10-708); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *FCC v. AT&T Inc.*, 131 S. Ct. 1177 (2011); *Doe v. Reed*, 130 S. Ct. 2811 (2010); *Flores-Figueroa v. United States*, 556 U.S. 646 (2009); *Crawford v. Marion Cnty. Election Bd.*, 553 U.S. 181 (2008); *Hiibel v. Sixth Judicial Circuit of Nev.*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Dep't of Justice v. City of Chi.*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002); *Reno v.*

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Condon, 528 U.S. 141 (2000); *IMS Health Inc. v. Sorrell*, 630 F.3d 263 (2d Cir. 2010); *IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) *cert. denied,* 129 S. Ct. 2864 (2009); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006); *Gonzales v. Doe*, 449 F.3d 415 (2nd Cir. 2005); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); *Commonwealth v. Connolly*, 913 N.E.2d 356 (Mass. 2009); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a particular interest in ensuring that workplace privacy is not diminished as the use of new communications services increases. *See* Brief of *Amici Curiae* Electronic Privacy Information Center (EPIC) et al. in Support of Respondents, *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2610 (2010) (No 08-1332) (concerning the privacy of text messages). Employees in the modern "workplace," which may be at home or on the road, frequently use communications devices to send both work and non-work related messages. In some circumstances, employers may be able to fairly limit some expectations of privacy in those communications, but such policies cannot overcome well-established rules of privilege nor can they be applied retroactively, as the confidentiality of a privileged communication must be measured at the time the communication was made.

SUMMARY OF THE ARGUMENT

This case presents an important issue: the application of federal evidentiary privilege to communications in the workplace. The daily activities of employees generate numerous records – voicemails, emails, text messages, and even "tweets" – that contain both public and private information. An employee's expectation of privacy in particular communications may not always be clear, but courts have recognized such privacy rights in the Fourth Amendment context, *see, e.g., City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010); *O'Connor v. Ortega*, 480 U.S. 717 (1987), and confidentiality protections in the federal privilege context. *See, e.g., In re Teleglobe Commc'ns Corp.*, 493 F.3d 345 (3d Cir. 2007); *United States v. Barrows*, 481 F.3d 1246 (10th Cir. 2007); *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010); *Banks v. Mario Industries of Virginia, Inc.*, 274 Va. 438 (2007).

The decision below set out a broad and unprecedented holding that an individual's reasonable expectation of privacy in personal communications with a spouse could be retroactively waived by a workplace use policy. This ruling implicates an enormous range of employee activity, including all personal communications sent over a work computer or similar device, and threatens to diminish well-established privileges that foster candid communications between spouses and other groups.

The retroactive application of a workplace use policy in this case is especially problematic given the nature of digital records. Employees will be put in an impossible situation if they rely on the absence of a policy to make an informed decision about the use of a workplace communications service, and are then required to act *after* a change in policy with respect to their *prior* communications. Such a practice could lead to the unfair collection of not only marital communications but attorney-client records, sensitive medical records, and other potentially privileged materials that are routinely stored in digital form and transferred confidentially over the Internet.

ARGUMENT

Communications between spouses, in particular, implicate important privacy and confidentiality interests that are embodied in the federal common law marital privilege. The marital communications privilege, under which communications between spouses are presumptively confidential, was first recognized by the Supreme Court in 1934. Mikah K. Story, *Twenty-First Century Pillow-Talk: Applicability of the Marital Communications Privilege to Electronic Mail*, 58 S.C. L. Rev. 275, 278-79 (2006); *Wolfe v. United States*, 291 U.S. 7 (1934). The privilege "reaches those marital communications made in confidence and intended to be confidential." *United States v. Poole*, 451 F. App'x 298, 307 (4th Cir. 2011). This common-law marital privilege is incorporated through Federal Rule of

Evidence 501 and has been codified "in forty-nine states and the District of Columbia." *See* Story, *supra*, at 281-82.

The decision reached by the court below, holding that an individual has no reasonable expectation of privacy in e-mails sent from a workplace computer at a time when the employer had no acceptable use policy in place, is unprecedented. No other court has held that such a workplace use policy can be applied retroactively to alter the private and confidential nature of communications sent before it was implemented. In fact, a majority of courts consider the existence of a use policy to be a "necessary but not sufficient" element to establish waiver of privilege. Adam C. Losey, Note, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 Fla. L. Rev. 1179, 1192 (2008). To hold otherwise would be contrary to the Supreme Court's clear statement in *O'Connor* that "the question of whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." *O'Connor*, 480 U.S. at 718. The retroactive application of workplace use policies, which are subject to change without notice, would place an unreasonable burden on employees to audit all potentially private or privileged records. Even if an employee knew that a particular record should be deleted, there may be no available means to do so once it has been created.

This Court should recognize the importance of workplace privacy and consider the far-reaching implications of the lower court's decision limiting employees' reasonable expectation of privacy in personal communications.

I. Because the Distinction Between Business and Personal Communications is Eroding, a Workplace Use Policy Alone Should Not Eliminate an Employee's Reasonable Expectation of Privacy in Personal Communications

Employers and employees are currently adapting to new communications devices as they become increasingly integrated into the home and workplace. More than fifty percent of adults were using a computer at work in 2003. Jennifer Cheeseman Day, Alex Janus & Jessica Davis, U.S. Census Bureau, Current Population Reports P23-208, *Computer and Internet Use in the United States: 2003*, at 12 (2005). Today nearly every office worker uses a laptop or desktop computer, e-mail, and Internet browser as part of their day-to-day job. WorldOne Research, *LexisNexis Technology Gap Survey* (Apr. 15, 2009).[2] Employees are increasingly using handheld and other devices "for a variety of reasons and often regardless of official company policies." Jeanne G. Harris, Blake Ives & Iris Junglas, *The Genie Is Out of the Bottle: Managing the Infiltration of Consumer IT*

[2] http://www.lexisnexis.com/media/pdfs/LexisNexis-Technology-Gap-Survey-4-09.pdf.

into the Workplace 4 (Accenture Institute for High Performance, Oct. 2011).[3]

Employees are using their own devices and devices provided by employers for both business and personal activities, at home and in the workplace. Accordingly, any workplace use policy will impact some personal, private communications. For the district court, the existence of a workplace use policy, *put in place after the fact,* declaring that employees "must not have and shall have no expectation of privacy" when using the Newport News Public Schools' network trumped the well-established privacy and confidentiality involved in a marital communication. Given the substantial privacy interests at stake, this Court should reject the analysis of the district court and hold that a workplace use policy is necessary, but not sufficient, to overcome an employee's reasonable expectation of privacy in personal communications.

A. Employees Regularly Use Computers and Handheld Devices, at Home and in the Office, for Personal and Work-Related Activities

For most employees, use of the Internet and email is a workplace necessity. *See* Qinyu Liao et al., *Workplace Management and Employee Misuse: Does Punishment Matter?*, 50 J. Computer Info. Sys. 49 (2009); Mary Madden & Sydney Jones, PEW Internet & Am. Life Project, *Networked Workers*, at i (2008)[4]

[3] http://www.accenture.com/us-en/Pages/insight-managing-infiltration-consumer-it-workforce.aspx.

[4] http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf.pdf

(fifty-three percent of American adults employed full- or part-time, sixty-two percent use e-mail or the Internet at work). Employers continue to provide more devices like cell phones, smartphones, and laptops to enable constant employee connectivity. *See* Janna Quitney Anderson & Lee Rainie, PEW Internet & Am. Life Project, *The Future of the Internet III* (Dec. 14, 2008).[5] A *USA Today* poll found that fifty-nine percent of professionals reported that their employer paid for the laptop they regularly use for work. Michelle Kessler, *Some Employees Buy Own Laptops, Phones for Work*, USA Today, June 16, 2008.[6] Fifty-six percent of professionals said that their employer paid for their smartphone. *Id.* Twenty-four percent said that their employer paid for their regular cell phone. *Id.* And 21% of employees surveyed said that their employer paid for their Personal Digital Assistant. *Id.*

Furthermore, technology has expanded the boundaries of the modern workplace, allowing employees to work beyond the four walls of the office. A recent Bureau of Labor Statistics survey found that 24 percent of employees did some or all of their work at home. Bureau of Labor Statistics, U.S. Dep't of Labor, *Work at Home and in the Workplace*, Editor's Desk (June 24, 2011).[7] Even office-

[5] http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_FutureInternet3.pdf.pdf.
[6] *Available at* http://www.usatoday.com/money/workplace/2008-06-15-electronic-devices-workplace_N.htm.
[7] http://www.bls.gov/opub/ted/2011/ted_20110624.htm.

based employees are capable of working outside the office. Modern smartphones can replicate many of the functions of many of the devices found in the office, enabling employees to send email, browse the web, make phone calls, and send text messages. *See, e.g.,* Apple, *iPhone: Built-in Apps*;[8] Blackberry, *Blackberry Smartphones*.[9] Over two-thirds of American workers report checking for work-related emails over the holidays. Mike Flacy, *Over Two-Thirds of Americans Check Work Email During Major Holidays*, Digital Trends (Nov. 28, 2011).[10] Thus, for an employee with a smartphone, the "workplace" could be located anywhere.

B. Employees Use These Devices for Personal Communications That Implicate Important Privacy Interests

For a variety of reasons, many employees use work-related devices for personal activities. *See* Jessica Vitak et al., *Personal Internet Use at Work: Understanding Cyberslacking*, 27 Computers Hum. Behav. 1751 (2011). Seventy-seven percent of US workers use Facebook at work, and the average amount of time spent on Facebook is 40 minutes. Nucleus Research, *Facebook Costs Companies 1.5 Percent of Total Productivity* (July 21, 2009).[11] Because of this,

[8] http://www.apple.com/iphone/built-in-apps/ (last visited Apr. 6, 2012).
[9] http://na.blackberry.com/eng/devices/ (last visited Apr. 6, 2012).
[10] http://www.digitaltrends.com/web/over-two-thirds-of-americans-check-work-email-during-major-holidays/.
[11] http://nucleusresearch.com/news/press-releases/facebook-costs-companies-1-dot-5-percent-of-total-productivity/.

any workplace use policy is almost certain to impact personal communications, such as the marital communications at issue in this case.

Complete segregation of business and personal uses is simply impractical. Even the most diligent employee does not spend every working second completing business tasks. Most employees say that they are not going to use or carry two cell phones or laptops, which makes the existence of strictly separate "business" and "personal" devices unlikely. *See* Michelle Kessler, *Some Employees Buy Own Laptops, Phones for Work,* USA Today, June 16, 2008. The erosion of the business-personal distinction has also been accelerated by the increasing adoption by businesses of personal collaboration and sharing tools. Cisco's WebEx solution and Skype, for example, are two technologies that were initially used for personal reasons but then became popular with businesses. *See* Abhijeet Rane & Tavishi Agrawal, *The Future of Workplaces* 6 (2011) ("Skype started off as a means to communicate personally with friends and relatives; businesses quickly absorbed it when employees found the service an extremely convenient way to be in touch with their co-workers and colleagues across cities and countries.").[12] Thus, from the employee's perspective, workplace devices are migrating into the personal

[12] *Available at* http://livingworkplace.skype.com/assets/pdf/Future_of_Workplaces-GigaOmPRO.pdf.

realm at the same time that products and services originally used for personal reasons are migrating into the business realm.

Individual privacy, such as the privacy of communications, is a fundamental human value. Privacy is necessary for personal autonomy, dignity, and respect. "Privacy," Professor Helen Nissenbaum writes, "frees us from the stultifying effects of scrutiny and approbation (or disapprobation), it contributes to material conditions for the development and exercise of autonomy and freedom in thought and action." Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 82 (2010). As Professor Julie E. Cohen describes, cognitive psychology research demonstrates that "lack of privacy makes people both less inclined to experiment and less inclined to seek help . . . . Individuals who experiment with unpopular views or behavior also must consider the possibility of physical, economic, or social sanctions." Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1425 (2000). Research shows that surveillance in the workplace reduces employee efficiency when performing difficult tasks. J.R. Aiello & C.M. Svec, *Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence*, 23 J. Applied Soc. Psych. 537 (1993). Professor Jeffrey Rosen has noted that employees "experience a dignitary injury when they are

treated like the inhabitants of the Panopticon." Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* 214 (2000).

Accordingly, in 1996, the International Labour Organization (ILO) adopted a code of practice on the protection of workers' personal data. See Int'l Labour Organization, *Protection of Workers' Personal Data* (1997).[13] The ILO code is the respected international standard on the protection of workers' privacy rights. The code specifies that workers' data should be collected and used consistently with Fair Information Practices (FIPs). Importantly, notice of data collection is only one of the practices listed. The code also includes substantive limitations, such as:

- That employers should collect the minimum necessary data required for employment
- That data should only be used for reasons directly relevant to employment, and only for the purposes for which the data were originally collected
- That certain data, such as sex life and political and religious beliefs, should not be collected.

Id. If an employer monitored all employee email communications, regardless of context or content, it would violate several of these protections. Such blanket surveillance would gather more than the "minimum necessary data required for employment" and would likely result in the unnecessary collection of sensitive data.

[13] *Available at* http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

Email communications are also protected under a variety of federal statutes. The Wiretap Act prohibits the intentional interception of electronic communications. *See* 18 U.S.C. §§ 2511(1)(a). The Stored Communications Act prohibits unauthorized users from accessing e-mails and requires a warrant to search the content of e-mails that have been stored for 180 days or less. *See* 18 U.S.C. §§ 2701, 2703(a). In *Warshak v. United States*, the Sixth Circuit recognized that email communications are intended to be private. *See* 490 F.3d 455 (6th Cir. 2007), *vacated as not ripe for adjudication*, 532 F.3d 521 (6th Cir. 2008) (en banc).

Where, as here, the content of an email consists of information disclosed between a husband and a wife, the private nature of the communication cannot be denied. Indeed, privacy in marital communications is "regarded as so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails." *Wolfle v. United States*, 291 U.S. 7, 14 (1934); *see also United States v. Parker*, 834 F.2d 408, 411 (4th Cir. 1987). Thus, marital communications are "generally assumed to have been intended to be confidential." *Wolfle*, 291 U.S. at 14.

These types of personal communications, unrelated to any business activity, do not give rise to the same risks and concerns motivate employers to institute workplace use policies in the first place. Employers are rightfully concerned about

employees sharing confidential or proprietary business information, including intellectual property and trade secrets, or sending obscene and offensive material that could give rise to liability. *See* Proofpoint, *Outbound Email and Content Security in Today's Enterprise* 2 (2006) (summarizing the results of a survey of corporate policies and motivations related to the monitoring of email).[14] But employers cannot use the same rational to justify monitoring of personal messages unrelated to work. This is an important distinction to make when analyzing waiver of privilege, because the most difficult cases arise from workplace e-mails that implicate the employer-employee relationship. *See, e.g., Banks v. Mario Industries of Virginia, Inc.*, 274 Va. 438 (2007) (former employees sued for forming competing business while still working for employer).

This problem arises not only in the context of personal communications between a husband and wife, but also in the context of confidential professional activities in a shared workplace. A recent article described the particularly vexing problem of a law professor's use of University facilities to provide legal services to clinical clients, pro bono clients, and outside law firms. *See* Gregory C. Sisk & Nicholas Halbur, *A Ticking Time Bomb? University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings*, 2010 Utah L. Rev. 1277 (2010). Any bright-line rule adopted undermining the confidentiality of e-mails

[14] http://www.proofpoint.com/downloads/Proofpoint-Outbound-Email-and-Content-Security-2006.pdf.

sent from the workplace would create severe ethical implications for law professors and other legal professionals who work in mixed-use offices. Perhaps it makes more sense to limit the scope of workplace use policies when they are at odds with so many well-established legal and ethical norms (privilege, confidentiality, and the attorney-client relationship).

C. This Court Should Hold That the Mere Presence of a Workplace Use Policy is Not Sufficient to Defeat the Reasonable Expectation That Employees Have in the Privacy of Their Personal Communications

The district court concluded that the NNPS log-on banner negated both an objectively reasonable expectation of privacy and a claim of marital privilege in the content of defendant's stored emails. *United States v. Hamilton*, 778 F. Supp. 2d 651, 654, 655 (E.D. Va. 2011). Given the erosion of the personal-business distinction with new communications technologies, the lower court's approach should be rejected. Under that approach, the mere existence of a workplace use policy could unreasonably diminish the privacy of personal communications sent between spouses, or other protected groups, while the employees are not at work or even engaging in work-related activities.

Other courts have adopted a different approach, under which the existence of a workplace use policy is necessary, but not sufficient, to render an expectation of privacy unreasonable. In *In re Asia Global Crossing*, the Bankruptcy Court for the Southern District of New York developed a four-part test to measure the

expectation of privacy in emails sent by company employees to their attorneys using the company's email system: (1) whether the employer maintained a use policy, (2) whether the employee's computer or e-mail were actually monitored, (3) whether third parties had a right to access the employee's computer or e-mail, and (4) whether the employee was notified or aware of the policies. 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005). The *Asia Global* test has been cited by courts within this circuit. *See Sprenger v. Rector,* No 07-502, 2008 WL 2465236 (W.D. Va. June 17, 2008); *Hanson v. First Nat'l Bank*, No. 10-0906, 2011 WL 5201430 (S.D.W. Va. Oct. 31, 2011).

In *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court supplemented the *Asia Global* factors with others derived from caselaw, including (1) the clarity and scope of the workplace use policy itself; (2) whether the employee communicated using his personal email account or the workplace account; (3) the extent of personal use of employer equipment permitted by the employer; (4) the location of the employer's equipment; and (5) the presence of government actors. 201 N.J. 300, 314-21 (2010). The court also considered the "important public policy concerns raised by the attorney-client privilege." *Id.* at 314. Importantly, the court adopted a pragmatic view toward the nature of the modern workplace. *Id.* at 320 ("We recognize that a zero-tolerance policy can be

unworkable and unwelcome in today's dynamic and mobile workforce and do not seek to encourage that approach in any way.").

This Court should reject the single-factor analysis employed by the court below. Consideration of additional factors, outlined in the cases above, is necessary given the strong privacy interest in spousal communications.

II. An Acceptable Use Policy Cannot Retroactively Alter an Employee's Reasonable Expectation That Personal Communications Are Private

The question of whether an individual reasonably believed that a communication was private must be determined at the time the communication was made. Edward J. Imwinkelried, *The Dangerous Trend Blurring the Distinction Between a Reasonable Expectation of Confidentiality in Privilege Law and a Reasonable Expectation of Privacy in Fourth Amendment Jurisprudence*, 57 Loy. L. Rev. 1, 13 (2011); Edward J. Imwinkelried, *The New Wigmore: Evidentiary Privileges* § 6.8.1 (2d ed. 2010). *See United States v. Inigo*, 925 F.2d 641, 657 (3d Cir. 1991); *Costal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 863 (D.C. Cir. 1980). Any rule that allows the privacy of a communication to be waived by a new workplace use policy, put into place after the communication occurred, would impose an unreasonable burden on employees.

This is not a traditional case of waiver where an individual affirmatively acted to disclose materials. This is not even a case of implied waiver where an

individual negligently failed "to take adequate precautions to maintain their confidentiality." *SEC v. Lavin*, 111 F.3d 921, 930 (D.C. Cir. 1997). The employee here acted as any reasonable employee would. It would be extreme to find that "adequate precautions" require an employee to scan all archived e-mails and remove any that are personal and confidential every time the workplace use policy changes. In fact, employees may not even be aware that archived e-mails exist or know where to find them. Even if an employee was able to identify such an e-mail, he may not be able to adequately and permanently delete it.

A. Workplace E-Mails Are Stored by Default, and Employees May Not Know How or Where to Delete Them

Enterprise e-mail systems can be managed on-site or remotely (in the cloud). *See generally* Osterman Research, Inc., *Why the Cloud is Not Killing Off the On-Premises Email Market* (April 2011).[15] An on-site corporate system typically consists of a server (or servers) configured to deliver e-mail and other file services. *See* Frank Ohlhorst, *SAAS or On-Premise Email: Which is Best?*, Channel Insider – Message & Collaboration (Feb. 3, 2009).[16] Cloud-based systems are hosted on remote servers and can be accessed over the Internet. *Id.* Regardless of the technology used, the end user experience is the same: e-mail messages are sent and

[15] http://www.sendmail.com/pdfs/whitepapers/Why_the_Cloud_is_Not_Killing_Off_On-Premises_Email_Sendmail.pdf.
[16] http://www.channelinsider.com/c/a/Messaging-and-Collaboration/SAAS-or-OnPremise-Email-Which-is-Best/1/.

received through a client application, referred to as a Mail User Agent ("MUA"). *See* Kavi Corporation, *Mailing List Manger Help – Chapter 7. How Email Really Works* (2008).[17] The e-mail server receives incoming messages and delivers them to the user's MUA, at which point they are stored on the server, the user's device, or both. *See* Microsoft, *Outlook 2003 Help and How-to: Leave E-mail Messages on Your E-mail Server*.[18]

Incoming and outgoing e-mails are stored by default, not deleted. On an employee computer, archived messages are typically stored in a data file on the local hard drive. *See, e.g.,* Microsoft, *Outlook 2010 Help and How-To: Where Does Microsoft Outlook 2010 Save My Information and Configurations?*.[19] Current e-mail files are also stored on the workplace server in the most common configuration. *Id.*; The Radicati Group, Inc., *Microsoft Exchange Server and Outlook Market Analysis, 2012-2016* (Sara Radicati, PhD, Mar. 2012) (showing a 53% worldwide penetration of Microsoft Exchange Server in the Enterprise Messaging market in 2012). Even if archived messages are stored locally on the employee's machine, the employee might not know where the file is located, or might not know how to properly delete the file. *See*, *infra*, at Part II.B.

---

[17] http://www.niso.org/khelp/kmlm/user_help/html/how_email_works.html
[18] http://office.microsoft.com/en-us/outlook-help/leave-e-mail-messages-on-your-e-mail-server-HA001150793.aspx (last visited Apr. 3, 2012).
[19] http://office.microsoft.com/en-us/outlook-help/where-does-microsoft-outlook-2010-save-my-information-and-configurations-HP010354943.aspx.

Current server software enables automated message archiving and retention without affecting the end-user's experience; the result is that the user has less control over where the messages are stored and when they are deleted. *See* Microsoft, White Paper, *Addressing E-mail Archiving and Discovery with Microsoft Exchange Server 2010* ("To help deliver a familiar user experience, the Personal Archive appears alongside primary mailbox").[20] As these settings and interfaces change, employees will continue to face "user confusion," and may inadvertently retain logs and messages that they intended to delete. *See* Michael Jones, *Prevent Spotlight From Resurrecting Your Deleted Emails on iPhone*, Túaw (Aug. 18, 2009) ("When you delete an e-mail message in most mail clients, the message isn't magically deleted, but instead moved to a 'trash' or 'deleted messages' folder.").[21] The problem of user confusion is even more acute with advanced handheld devices, which are configured in such a way that the user does not know whether messages are stored locally, on the cloud, or both.

[20] *Available at* http://www.microsoft.com/exchange/en-us/email-archiving-and-retention.aspx (last visited Apr. 04, 2012).
[21] http://www.tuaw.com/2009/08/18/prevent-spotlight-from-resurrecting-your-deleted-emails/.

B. Even When Employees Take Extra Precautions and Delete Private Communications, They Cannot Be Sure They Are Not Recoverable

"[E]mails are like the cockroach of the electronic world … very difficult to get rid of." Interview by Steve Inskeep with Elizabeth Charnock, CEO, Cataphora, *Investigating Employees' E-Mail Use*, NPR – Morning Edition (Jun. 18, 2008).[22]

Workplace computers store a wide range of sensitive information about employees. *See*, *supra*, Part I.B. If a document or message is especially private or important, an employee might attempt to delete it or otherwise protect it. However, unless the employee has special computer expertise, he is unlikely to truly "delete" any record in a way that makes it inaccessible and unrecoverable. *See* Adam C. Losey, Note, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 Fla. L. Rev. 1179, 1191-92 (2008) (discussing the difference between 'single deleting' and 'double deleting' documents). The result is that a reasonable effort by an employee to maintain the privacy of a document or communication is frustrated by technology. This is a real and persistent threat to employees who engage in private communications throughout the day that may or may not be transferred over employer-provided devices.

The law on waiver of privilege in the workplace is far from settled, but cases make clear that waiver requires a clear policy in place at the time the document was created. In a recent Virginia case, *Banks v. Mario Industries of Virginia, Inc.*,

[22] *Available at* http://www.npr.org/templates/story/story.php?storyId=91625695.

274 Va. 438 (2007), an employee used his work computer to prepare a pre-resignation memorandum. *Id.* at 453. He printed the memo from his work computer and then deleted it, but it was later recovered by his employer's "forensic computer expert." *Id.* at 454. The Virginia Supreme Court held that the existence of an employee handbook, at the time the document was created, specifying there was "no expectation of privacy" regarding workplace computers was sufficient to waive attorney-client privilege. *Id*.

Even the approach adopted by the Virginia Supreme Court in *Banks* would not apply retroactively to documents and messages created before the use policy was put into place. Employees are unlikely to delete messages in a way that makes them unrecoverable. In fact, the use of tools to "clean" and "wipe" personal files can cause major problems for the employee and the employer if litigation ever arises. *See* Craig Bell, *Double Delete Doesn't Do It*, L. Tech. News (Apr. 1, 2011).[23] An employee may "unwittingly destroy discoverable data while intentionally destroying irrelevant (usually personal) data, [and] courts are unlikely to afford the bad actor (or his employer) the benefit of the doubt." *Id*. Thus, the employee is put in an impossible position when his employer alters its use policy and threatens the privacy of pre-existing documents and communications. The

[23] http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202487043726&slreturn=1.

employee cannot delete the files in a way that is secure and permanent without risking potential liability or prejudice by inadvertently erasing discoverable data.

C. Employees Should Not Bear the Burden of Re-Assessing the Protection of Private Documents and Communications Every Time the Use Policy Changes

The average employee uses a variety of devices to complete both personal and professional tasks. At times these activities may be discrete and easily segregable, but inevitably there will be some overlap. The privacy of employee records and communications is increasingly complicated due to the convergence of personal and workplace devices. It becomes even more complicated as workplace use policies change over time. The addition of new devices and novel legal standards, as well as normal institutional adjustment, will require continual changes in these policies over time. It would be unfair and unrealistic to expect employees to audit their private records each time the policy changes. Courts should not draw distinctions that prejudice employees without leaving them a viable alternative.[24]

The current case is a prime example of this problem in action. Mr. Hamilton communicated with his wife in private via e-mail in 2006 from his NNPS account. *United States v. Hamilton*, 778 F. Supp. 2d 651, 652 (2011). A year later, NNPS instituted an acceptable use policy that allowed monitoring of communications and

[24] Consider the implication of this retroactive waiver. Would the result change if the new policy had been implemented the day before the files were seized?

inspection of files. *Id.* at 652-53. How was Mr. Hamilton to protect his private communications after the new policy was announced? If the archived e-mails were stored locally on his work computer, he could delete them. But, even if he attempted to delete the files, they would likely be stored on the e-mail server or otherwise recoverable by a computer forensics expert. If he attempted to use advanced software to "wipe" the files from his computer, he might later be prejudiced in court if the files were considered discoverable.

The decision adopted by the court below is contrary to the law of federal evidentiary privilege, fails to recognize the widespread use of modern communications services for both work and non-work purposes, and adopts an unprecedented application of "retroactive waiver." As a result, employees are put in an impossible situation, unable to protect their personal information even when their expectation of privacy is well established in law and by custom.

CONCLUSION

Amicus respectfully requests this Court to grant Appellant's motion as to Issue II and hold that the trial court erred in allowing into evidence e-mails between Defendant Hamilton and his wife.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 5,210 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14 point Times New Roman style.

Dated: April 6, 2012

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of April 2012, the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Appellant and Urging Reversal was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties *via* electronic delivery.

Dated: April 6, 2012

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140