JOURNAL OF INTERNET LAW
VOLUME 13
NUMBER 8
ASPEN PUBLISHERS
FEBRUARY 2010
EDITED BY DLA PIPER

The Increasing Privacy Expectations in Employees' Personal Email

By Marjorie J. Peerce and Daniel V. Shapiro

Technology is transforming the working world. Mobile email devices and remote access have lengthened the working day and further blurred the distinction between business and personal time. As a result, both employers and employees have changing expectations about work. Employers now expect that employees are always reachable.[1] In addition, employees have come to expect access to the Internet for personal use at work.[2] Some employees use their company email accounts for personal business, and some use their personal email accounts for company business.[3] This use of both work email and personal Web-based email, all while on company equipment, has raised complex questions regarding privacy expectations in the changing workplace.

As employees log on to personal Web-based email accounts, they frequently leave login credentials and temporary Internet files on a company computer. What employees may not realize is that anything that they view or send over the Internet (even if the employee is using a personal account) may be accessible to third parties by accessing these temporary Internet files on the company computer used by the employee. This record of activity, potentially including the username and password for the employee's personal Web-based email account, remains stored on the company computer unless manually erased. And, even then, the record can frequently be recovered. Even an employee using a company laptop at home, accessing the Internet through his own service provider, creates a record of his activity on the company's computer.

So what happens when there is a legal need to review the material on company computers,

Continued on page 14

Marjorie J. Peerce *(mpeerce@stillmanfriedman.com) is a member at Stillman, Friedman & Shechtman, P.C. (www.stillmanfriedman.com).* **Daniel V. Shapiro** *(dshapiro@stillmanfriedman.com) is an associate at the firm.*

IN THIS ISSUE

THE INCREASING PRIVACY EXPECTATIONS IN EMPLOYEES' PERSONAL EMAIL 1
By Marorie J. Peerce and Daniel V. Shapiro

REGULATING SPYWARE: CHALLENGES AND SOLUTIONS 3
By Daniel B. Garrie, Yoav Griver, and Mari Joller

ESTONIA THREE YEARS LATER: A PROGRESS REPORT ON COMBATING CYBER ATTACKS. 22
By Scott J. Shackelford

Wolters Kluwer
Law & Business

The Increasing Privacy Expectations
Continued from page 1

such as an internal investigation, employment dispute, or civil litigation? Can an employer view the temporary Internet files on the company computer? Can an employer log in to the employee's personal email account without the employee's consent? This article reviews some of the current case law on these emerging issues, provides suggestions on best practices to minimize liability, and looks to electronic communications policies recently implemented by the federal government as a potential model for procedures to reduce exposure to civil and criminal liability.

These are not easy questions, and the law is evolving rapidly.[4] The developing case law suggests (1) that an employer can view the temporary Internet files on a company computer with the possible exception (in some jurisdictions) of privileged communication to the employee's attorney and (2) that an employer cannot log in to an employee's personal Web-based account. The restriction for Web-based accounts exists because they are protected from access by the Stored Communications Act (SCA). This differs from the law governing an employer's internal email system, which is generally understood to be under the ownership and control of the employer. Indeed, courts have found violations of the SCA by employers who log in to review their employees' Web-based personal accounts.[5] Other courts have suppressed evidence that an employer obtained in violation of the SCA.[6] In addition to the SCA, employers must be aware of the risks of reviewing privileged material. Some courts have found that email sent by an employee to his or her attorney, even if accessible in the temporary Internet files of a company computer, is still privileged.[7] Although some courts have found a waiver of the attorney-client privilege when the employee was on notice that the employer would be able to access a privileged email sent from a company computer, other courts are now holding that, even when on notice, there is no waiver.

For counsel tasked with conducting internal investigations, these developments create increasing complexities and uncertainties regarding the limits of what personal information can be retrieved from an employee's work computer and how that information can be used. The traditional employer protection of a broad electronic communications policy, which generally informs employees not to expect any privacy, is under assault by some courts. The risk from making the wrong decision is possible civil and even criminal liability. As we discuss in this article, court decisions that vary by jurisdiction only increase the uncertainty in this rapidly developing area of law.

EMPLOYEES ARE INCREASINGLY COMMUNICATING USING PERSONAL EMAIL

Because employees are increasingly using their personal Web-based accounts in addition to company email systems, information relevant to an investigation may reside in personal accounts that do not belong to an employer. This has implications for companies conducting internal investigations and for the government's ability to retrieve an individual's email. Traditionally, when an investigation that involves possible wrongdoing at a company is underway, the company frequently cooperates and turns over email and other evidence to the government to be considered a good corporate citizen. This often takes place without any notice or involvement from the employee.

When a Web-based email provider possesses the information, the issue is more complicated. Although a company may be able to review certain materials stored in the temporary Internet files of a company computer, it cannot lawfully access an employee's Web-based email account without authorization, even if it lawfully discovered the login credentials. This is because the SCA provides for possible criminal and civil action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided."[8]

While an employer cannot access information from a Web-based provider, the government can obtain such records from a provider of electronic communications services using formal procedures under the SCA. For communications that have been in storage for 180 days or less, the government's only option is to obtain a search warrant.[9] If the communication has been in storage for more than 180 days, the government may either (1) obtain a search warrant for the communication or (2) use an

administrative subpoena, grand jury or trial subpoena, or court order to obtain the information.[10] If the government uses a search warrant, no notice to the customer is required.[11] If the government employs a subpoena or court order, notice to the customer is required.[12] However, the government can make an application to delay that notice for good cause.[13] These added procedural requirements may give an individual the ability to challenge the relevant search warrant, court order, or subpoena.

Liability under the SCA poses a significant risk to an employer exceeding its authorized access to an employee's email account.

This shift in procedure when an email resides with a Web-based email provider can have significant consequences. A recent example is the securities fraud prosecution of former Bear Stearns hedge fund managers Ralph Cioffi and Matthew Tannin, where a dispute arose over the admissibility of emails allegedly sent by Tannin through his personal Gmail account. According to the opinion, the search warrant that the government obtained "did not, on its face, limit the items to be seized from Tannin's personal email account to emails containing evidence of the crimes charged in the indictment, or, indeed, any crime at all."[14] As a result "[i]t was, therefore, unconstitutionally broad."[15] The court excluded the email and declined to allow the government to try to remedy the problem by obtaining a new search warrant with the requisite particularity, finding that there was "no way to purge the taint of [the government's] unconstitutionally overbroad search."[16] Cioffi and Tannin were ultimately found not guilty on all counts.

Ten years ago, it was more common for employees to send all of their work-related email from a company account, thereby enabling the company to turn it over to the government as a good corporate citizen. But, as Web-based accounts increase in number and usage, more and more possibly relevant evidence will reside in Web-based accounts "in the clouds" and not on company servers.

What does a company do when it is conducting an internal investigation without the power the government has to issue such search warrants or subpoenas? It is crucial that companies understand the potential liability to which they may expose themselves for exceeding their authorization to review employee emails.

LIABILITY UNDER THE STORED COMMUNICATIONS ACT

Liability under the SCA poses a significant risk to an employer exceeding its authorized access to an employee's email account. The SCA creates a criminal offense and civil liability for anyone that "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and by doing so "obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[17] The SCA has been used to prosecute email hackers in the past, such as the college student who allegedly hacked into Sarah Palin's email account, and there is also a portion of the statute that creates a private cause of action through which a plaintiff can recover damages, including punitive damages if the violation "is willful or intentional."[18]

A computer that accesses a Web-based account merely provides a window into an account that is physically stored elsewhere. Information viewed or created using a company computer may be accessible without logging in to the account by accessing temporary Internet files on the company's computer. These temporary Internet files are arguably fair game to review with the exception that, in some jurisdictions, attorney-client communications cannot be reviewed. Other information in the account that was not viewed or created from a company computer, however, is likely accessible only by logging in and exploring the Web-based account using the credentials that the company discovered on the company computer. How far can one go?

This past March, the Fourth Circuit held—for the first time anywhere—that a plaintiff suing under the SCA for unauthorized login to her personal Web-based email account could recover punitive damages even in the absence of actual damages.[19] In *Van Alstyne v. Electronic Scriptorium Ltd.*, the plaintiff sued her former employer for sexual harassment. The employer then sued her in a separate action for business torts. During discovery, Van Alstyne became

suspicious that emails produced by her former boss were from her personal AOL email account, an account that she had used, in addition to her company account, to conduct business while employed at the company. The former boss admitted that he had logged in to Van Alstyne's AOL account numerous times from work, home, and while traveling. The jury awarded Van Alstyne more than $400,000 in damages and costs. On appeal, the Fourth Circuit struck down a portion of the award, but held that punitive damages may be awarded under the SCA even absent any showing of actual damages.

If, as *Van Alstyne* suggests, logging into a personal Web-based account can subject an employer to punitive damages, could it also subject that individual to criminal charges for the same "willful or intentional" conduct? The statute seems to suggest that it could. For this reason, *Van Alstyne* warrants the attention of counsel tasked with conducting internal investigations and creates potential headaches in an already unclear area of law.

LOOK, BUT DON'T LOG IN TO PERSONAL WEB-BASED ACCOUNTS

So how can an employer determine the extent to which it has been authorized to access an employee's Web-based account? Any analysis of an employee's expectation of privacy—and the authorization granted by the employee waiving that privacy—generally begins with a close reading of the company's electronic communications policy. In one recent case, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, a federal court in the Southern District of New York grappled with this issue and provided some guidance on the limitations of company searches.[20] The court ultimately excluded smoking gun evidence in the case because it was obtained in excess of the employer's authorization to access an employee's Web-based email account.

In *Pure Power Boot Camp*, the court suppressed evidence because it was obtained in violation of the SCA.[21] The facts alleged in *Pure Power Boot Camp* illustrate what an employer should not do, such as allegedly using information stored on a company computer to log in to a former employee's personal Web-based account and logging in to that employee's email account at his new job by guessing at his login and password.The court found that these actions exceeded the employer's authorization under the SCA.

Pure Power Boot Camp involved an alleged violation of a non-compete agreement. Alexander Fell and Ruben Belliard were both employed at a physical fitness center and were supervised by Lauren Brenner. Fell and Belliard left the company and opened a competing fitness center. After both Fell and Belliard had left the company, Brenner allegedly accessed three of Fell's personal Web-based email accounts for a period of one week. The opinion discloses that Brenner was able to access the three accounts (a Hotmail account, a Gmail account, and the account at the newly formed fitness center) because Fell had saved his Hotmail username and password information on the company's computers, allowing anyone going to the Hotmail Web site to be automatically logged in to his account. Brenner gained access to the Gmail account because the username and password had been sent to Fell in an email to his Hotmail account. Finally, Brenner was able to gain access to the new corporate account by guessing correctly that the username and password were the same as those used for the other two accounts.

No forensic examination of the company computer's temporary Internet files was ever conducted to determine which, if any, of the emails were created, received, sent, read, or accessed in any way from the company's computers. Fell testified that all of the emails were created or received on his home computer. Fell did not deny that he viewed some of his emails on company computers but did not identify any specific emails that he viewed. The emails that were recovered by Brenner turned out to be particularly relevant, containing an alleged admission that Belliard had destroyed the copy of his non-compete contract stored in Brenner's office (which prohibited him from forming his new business) as well as examples of Fell and Belliard's alleged attempts to steal clients.

Brenner claimed authorization to access Fell's emails because (1) the company's electronic communications policy put Fell on notice that his emails could be viewed, and (2) even if Fell had an expectation of privacy, he gave implied consent to access the accounts by leaving his username and password saved on the computer.

The court rejected the first justification by examining the relevant language of the company's

electronic communications policy, found in the company's Employee Handbook:

- [E]-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system. This includes the use of personal e-mail accounts on Company equipment. The Company, in its discretion as owner of the E-Mail system, reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through the system, for any reason, without the permission of any system user, and without notice.
- Internet access shall not be utilized for shopping or for conducting other transactions or personal business matters.[22]

The court concluded that the policy was limited to "Company equipment" and was limited to "any matter stored in, created on, received from, or sent through [the company's] system."[23] The email maintained by Google or Microsoft was therefore outside of the coverage of the policy because no evidence was presented that the emails at issue were created on, sent through, or received from company computers. Because no forensic analysis was conducted to see if any of the emails resided in the temporary Internet files of the computer, the company was unable to rely upon this language in the policy. If the emails had been recovered by a forensic examination of the temporary Internet files, instead of by logging in and exploring the Web-based account, the court may have found that the action was authorized.

The second justification advanced—that storing login credentials is the equivalent of implied consent—was also rejected. The court found that the company's policy permitted the company to search a company computer's files, but not log in and explore the Web-based account. Further, because there was no evidence that the Web-based account was used for work purposes or paid for by the company, an expectation of privacy remained. The court further rejected the notion that "if an employee simply views a single, personal e-mail from a third party e-mail provider, over [company] computers, then all of [] his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection."[24] Here again, the court drew a line between searching the employee's physical computer and using information found on that computer to log in to an email account.

In finding the employee's expectation of privacy reasonable, the court reviewed three factors in determining Fell's expectation of privacy:

1. Did the employee have a subjective belief that the material would be private?
2. Was that expectation reasonable, in part based on the electronic communications policy in place at the company?
3. Was the electronic communications policy clearly communicated to company employees or was it consistently enforced in a manner that would have alerted employees to the possibility that their private e-mail accounts could also be accessed and viewed by their employer?[25]

The court found that implied consent would not exist to access a Web-based personal account even when an employer has obtained access to the login credentials to the personal account because they were stored on the company's computers. Instead, the court compared the situation to a more traditional scenario: "[H]ad the person rummaging through the belongings in Fell's house found the key to Fell's country house, could that be taken as authorization to search his country house. We think not."[26] The court went even further to "reject[] the notion that carelessness equals consent."[27]

According to the court, implied consent requires "clear notice that one's conduct may result in a search being conducted of areas which the person has been warned are subject to search."[28] Implied consent did not exist in this case because, while Fell had notice that company computers could be searched for evidence of personal email use, he did not have notice that Web-based accounts would also be searched. Similarly, the court rejected as even more far-fetched the employer's argument that "guessing" someone's password amounts to authorization to access an account because it was in "direct conflict with the entire purpose of the SCA and basic principles of privacy."[29]

BE CAUTIOUS OF PRIVILEGE; IT CAN TRUMP A COMMUNICATIONS POLICY

To make things more difficult, even a company whose electronic communications policy permits

review of anything stored on a company computer can run into problems if attorney-client communications are reviewed. In the arena of privilege waiver analysis, courts have split on the issue of whether an employee waives the attorney-client privilege by sending or receiving privileged emails on a company computer. While some courts have held there to be a third-party waiver of privilege when employees were on notice that their employers would be able to access the privileged email sent from a company computer, other courts are now holding that, even when on notice, there is no waiver.

A recent New Jersey case illustrates how authorization may not exist even when the explicit wording of an employer's electronic communications policy indicates that the company should have authorization. In *Stengart v. Loving Care Agency, Inc.*, the issue was whether an employee's emails to her lawyer, recovered from the temporary Internet files on a company computer, which required no login but which were originally sent through her Web-based email account, were privileged.[30]

To resolve the question, the trial court reviewed the employer's electronic communications policy to determine whether the employee had a reasonable expectation of privacy in the email. In holding that the emails were not privileged, the trial court relied upon the fact that the Employee Handbook warned that "E-mail and voice mail messages, Internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee."[31] The trial court instructed that "the question of whether an employee has a reasonable expectation of privacy in a communication made on a work issued computer is based on the degree of notice the employer has provided to its employee regarding their right to privacy in electronic communications."[32]

On appeal, however, the New Jersey Superior Court, Appellate Division, reversed on the ground that the important societal interests underlying the attorney-client privilege trumped the company's electronic communications policy.[33] The Appellate Division held that, even if the terms of the electronic communications policy would have allowed the company to access the attorney-client communications, the privilege was still not waived on public policy grounds. The court found "little force in such a company policy when offered as the basis for an intrusion into the communications otherwise shielded by the attorney-client privilege."[34] This opinion joins other cases that extend the protection of privilege beyond its traditional reach and contributes to variances in third-party waiver law.[35] The case is currently under consideration by the New Jersey Supreme Court.[36]

The appellate court also found that, by examining the privileged emails, company counsel had violated New Jersey Rule of Professional Conduct 4.4(b), which requires a lawyer who receives a document that he realizes was inadvertently sent to avoid reading the document and promptly return it to the sender. The court acknowledged that "circumstances may arise when the attorney who has received such a document—whether through paper discover or by forensically examining a computer's hard drive—may arguably believe the document is not protected by the attorney-client privilege."[37] Even in that situation, the court held that the required course of action is "to cease reading or examining the document, protect it from further revelations, and notify the adverse party of its possession so that the attorney's right to retain or make use of the document may thereafter be adjudicated by the court."[38]

In the meantime, this ruling could create logistical problems in the context of an internal investigation when lawyers and paralegals working under incredible time pressures are reviewing thousands of emails. Must an employer contact the employee and turn over the document, thereby revealing the existence of the investigation? How can the privilege waiver issue be resolved if there is no pending case or proceeding? These issues will become more prevalent as employees use electronic media for every aspect of life, without fully understanding the traces that they leave behind.

GOVERNMENT EMPLOYEE EMAIL AS A MODEL FOR THE PRIVATE SECTOR?

A robust electronic communications policy coupled with signed acknowledgements from employees that they have reviewed the policy will go a long way toward protecting a company from liability under the SCA for searches conducted during an internal investigation. In addition to a written policy, however, it

is equally important that the statements and actions of company personnel do not contradict the stated policy. Recently, the Ninth Circuit held that a police officer maintained a legitimate expectation of privacy in the content of text messages that he sent and received on department equipment because his supervisor's informal guidance led him to believe that the department did not monitor text messages even though the official policy stated that it did.[39] But that may not be the final word, as the US Supreme Court has agreed to hear the case next term.

Any company that implements a strict communications policy must comply with it across the board if it wants the policy to have its intended effect.

Company communication policies, however, generally have not evolved as rapidly as technology. They therefore do not generally address the expectations that an employee should have about whether an employer can log in to the employee's personal accounts using a username and password that the employee has typed on a company computer and thereby inadvertently "shared" with the employer. Policies similar to the one in *Pure Power Boot Camp* are likely not explicit enough to allow a company to use an employee's recorded login information to access the employee's Web-based account. Although the typical policy makes clear that no communication should be considered private, it makes no reference to the company's ability to use the employee's login to obtain information that does not reside on the company's own computer network.

One option is to make the authorization explicit in a company's policy. Unchecked expansion of electronic communications policies, however, may not be in a company's best interest. As policies become more onerous and invasive, they may hinder a company's ability to recruit or retain talent. And, any company that implements a strict communications policy must comply with it across the board if it wants the policy to have its intended effect. If executives at the company regularly disregard the policy with no consequence, the company may lose its power to properly set employees' privacy expectations and thereby protect the company's review of an employee's electronic communications down the road.

But, if a company intends to implement such a change, how far-reaching and explicit does an electronic communications policy need to be to grant authorization to review Web-based accounts and privileged communications? A recent program implemented by the federal government to prevent security breaches provides some examples of the procedure that the government has used to inform employees that this computer use was being monitored. With some additions, these procedures could help a company strengthen its electronic communications policy.

The Department of Homeland Security has created an intrusion-detection system known as EINSTEIN 2.0 to prevent attempts to break into civilian unclassified federal computer systems.[40] This program, if fully implemented, would monitor email communications of federal employees and keep copies temporarily stored for analysis. The government has put user agreements and logon banners into place to comply with existing federal and state laws. These precautions could serve as models for companies trying to strengthen their electronic communications policies. The government's position is that:

> [b]y clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, an Executive Branch employee gives *ex ante* permission to the Government to intercept, monitor, and search "any communications" and "any data" transiting or stored on a Government-owned information system for any lawful purpose" and that this permission "necessarily includes the interception, monitoring, and searching of all personal communications and data sent or received by an employee using that system...."[41]

A logon banner is an agreement that appears on the screen when an employee logs in that the employee must agree to before he is permitted to use the computer. Under the government's plan, whenever a federal civilian employee logs in to the system he would see a variation of the following message:

- You are accessing a U.S. government information system, which includes (1) this computer, (2) this computer network, (3) all computers

connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.
  - At any time, and for any lawful government purpose, the government may monitor, intercept, and search any communication or data transiting or stored on this information system.
  - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.[42]

Before continuing, the user must click a button stating "I AGREE." In addition, all employees must sign a computer-user agreement that contains the same terms as the logon banner, except that it requires the employee to sign a document stating that the employee "understand[s] and consent[s]" to the foregoing terms.[43]

Companies already using computer-user agreements could strengthen their electronic communications policy through the use of logon banners as adopted by the government. Although the government program does not address the use of recovered login credentials, a company that wishes to extend its policy to cover such data could state in the logon banner and computer-user agreements that the employee agrees that the company has the right to use any login information entered on a company computer to log in and view messages in a personal account. Similarly, companies could include a provision that employees should not communicate with counsel using the company's computer systems because such communication is monitored and may waive any privilege that would otherwise attach to the communication. Finally, companies may further reduce their employees' expectations of privacy by prohibiting personal use of company computers and by explicitly stating in the policy that an employee's Internet activity is recorded on company-issued equipment and that any content viewed on the computer is available to the company for review. The question remains open how employees and the courts would react to such an explicit attempt to restrict employee privacy.

CONCLUSION

Underlying the emerging case law is a sense that the technologies at issue have evolved faster than the average employee or employer understands them. As one judge recently stated:

> Much of the reluctance to apply traditional notions of third party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not.[44]

The average employee does not fully understand that he or she may leave behind usernames and passwords when he or she logs in to his or her personal accounts on company computers or that the emails he or she sends to personal counsel may be cached locally on a company computer. Similarly, it is difficult for employers to understand what they can review without repercussions. As employees become more sophisticated and electronic communications policies become more plainly worded and specific, the pendulum may swing further toward employer authorization to review materials. Until that time, as *Van Alstyne*, *Pure Power Boot Camp*, and *Stengart* suggest, an employer is on safer ground when it remains within the boundaries of traditionally accepted practice and limits its review to non-privileged material accessible in the memory of the company's computers when its electronic communications policy provides authorization for such action. Even if a company has a novel electronic communications policy that explicitly allows for the use of login information or review of attorney-client communications, it should seek outside legal advice before acting in the present climate of uncertainty.

NOTES

1. *See* Shamus McGillicuddy, "Smartphones encourage users to work longer hours," *Mobile Computing* (Apr. 9, 2008), available at *http://searchmobilecomputing.techtarget.com/news/article/0,289142,sid40_gci1308971,00.html* (last visited Nov. 4, 2009) (survey found that individuals that have a smartphone work 71 additional minutes a day and that the average mobile user first checks his device at 7:10 a.m. and last checks it at 10:00 p.m.).
2. *See, e.g.*, Adam C. Losey, "Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege," 60 *Fla. L. Rev.* 1179, 1180 (2008), *citing* "Is That Work Related?," 24 No. 5 *Legal Mgmt.*, Sept.-Oct. 2005, at 8, 8 (average employee spends an hour a day on personal Internet use).
3. *See, e.g.*, Katie Hafner, "Putting All Your E-Mail in One Basket," *N.Y. Times*, June 26, 2003, at G1 ("It all becomes so intertwined, it's hard to know what's personal and what isn't.").
4. For example, it is possible that significant new case law has developed since this article went to print.
5. *See, e.g.*, Van Alstyne v. Electronic Scriptorium Ltd., 560 F.3d 199 (4th Cir. 2009).
6. *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (2008).
7. *See, e.g.*, Stengart v. Loving Care Agency, Inc., 973 A.2d 390 (Super. Ct. App. Div. 2009).
8. 18 U.S.C. § 2701.
9. 18 U.S.C. § 2703(a).
10. 18 U.S.C. § 2703(b).
11. *See* In the Matter of the Application of the United States for a Search Warrant for Contents of Electronic Mail, Nos. 08-9131-MC, 08-9147-MC, 2009 WL 3416240 (D. Ore. June 23, 2009) (holding that the Fourth Amendment does not require notice to the account holder when a search warrant is issued to a service provider for the contents of their e-mail).
12. 18 U.S.C. § 2703 (b).
13. Under 18 U.S.C. § 2705, the government may make an application to delay notice by a renewable 90-day period if there is a risk that disclosing the request may have an "adverse result," defined as "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(2).
14. United States v. Cioffi, No. 08-Cr-415 (FB), at 15 (E.D.N.Y. Oct. 26, 2009).
15. *Id.*
16. *Id.* at 20.
17. 18 U.S.C. § 2701.
18. 18 U.S.C. §2707(c).
19. Van Alstyne v. Electronic Scriptorium Ltd., 560 F.3d 199 (4th Cir. 2009).
20. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (2008).
21. *Id.*
22. *Id.* at 552-553.
23. *Id.* at 553.
24. *Id.* at 560.
25. *Id.*
26. *Id.* at 561.
27. *Id.*
28. *Id.*
29. *Id.* at 562.
30. Stengart v. Loving Care Agency, Inc., No. BER-L-858-08 (N.J. Super. Ct. Law Div. Feb. 05, 2009).
31. *Id.*
32. *Id.*
33. Stengart v. Loving Care Agency, Inc., 973 A.2d 390 (Super. Ct. App. Div. 2009).
34. *Id.* at *74.
35. *Compare* Convertino v. U.S. Dep't of Justice, Civ. No. 04-0236 (RCL) (D.D.C. Dec. 10, 2009) (no waiver when prosecutor emailed his attorney from his DOJ computers and personal use of the computers was not prohibited by policy) and Curto v. Med. World Commc'ns, Inc., No. 03CV6327, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. May 15, 2006) (no waiver for e-mails sent through a personal e-mail account on a company computer in employee's home) *with* Leor Exploration & Production LLC, et al. v. Aguilar, Civ. No. 09-60136 (JJO), 2009 WL 3097207 (S.D. Fla. 2009) (waiver when communications policy informed employee that computer use could be monitored) and Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, slip op. at 441-444 (N.Y. Sup. Ct. 2007) (waiver when employer email policy prohibited all personal use and allowed employer monitoring).
36. The Office of the Clerk for the Supreme Court of New Jersey summarizes the issue on appeal as follows: "under the circumstances presented, does the attorney-client privilege protect this employee's emails with her attorney sent through her personal, Internet-based email account while using her employer-issued computer?" *See* N.J. Courts Online, *Appeals Added in the New Jersey Supreme Court* (available at *http://www.judiciary.state.nj.us/calendars/sc_appeal.htm*) (last visited Nov. 5, 2009).
37. Stengart, 973 A.2d 390 at *75.
38. *Id.* at *76.
39. Quon v. Arch Wireless Operating Company, 529 F.3d 892 at 906-907 (9th Cir. 2008).
40. Memorandum from Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel (Jan. 9, 2009), available at *http://www.justice.gov/olc/2009/legality-of-e2.pdf* (last visited Nov. 3, 2009). *See also* Ellen Nakashima, "Cybersecurity Plan Doesn't Breach Employee Privacy, Administration Says," *Wash. Post*, Sept. 19, 2009, at A16.
41. *Id.*
42. *Id.*
43. *Id.*
44. *See* In the Matter of the Application of the United States for a Search Warrant for Contents of Electronic Mail, Nos. 08-9131-MC, 08-9147-MC, 2009 WL 3416240, at *13 (D. Ore. June 23, 2009).