A FOURTH AMENDMENT STATUS UPDATE: APPLYING CONSTITUTIONAL PRIVACY PROTECTION TO EMPLOYEES’ SOCIAL MEDIA USE

Alexander Naito*

INTRODUCTION

“Clauses guaranteeing to the individual protection against specific abuses of power, must have [the] . . . capacity of adaptation to a changing world.”¹

The transformation of the Internet over the past decade has dramatically altered the way business is conducted and how offices are structured.² File cabinets are being replaced in favor of electronic storage websites;³ letters have all but vanished as e-mail has become the preferred form of communication;⁴ and newspapers are on the ropes due in large part because blogs and other non-traditional on-

---

* Alexander Naito is a third year student at the University of Pennsylvania Law School and a Senior Editor of the Journal of Constitutional Law. This Comment benefited greatly from conversations with Tim Volpert of Davis, Wright, Tremaine LLP (Portland) and Steve Naito of Tarlow, Naito & Summers LLP. Most importantly, this Comment’s success is due in large part to the helpful edits and suggestions made by Linda Bartusiak and Professor Sophia Lee of the University of Pennsylvania Law School.

¹ Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J. dissenting).
² See 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, 898 (2005) (“In this era of information technology, where the fixed workplace is being rapidly displaced by a more protean electronic environment, wireless network connections create a seamless workplace. In a telecommuting world, an employee’s workplace may be anywhere and everywhere.”); David A. Couillard, Note, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2215–16 (2009) (describing how advancements in network technologies allows employees to work collaboratively from remote locations).
³ See Brandon Rowley, EMC Corporation (EMC) a Great Play on the Cloud, TRADING WALL ST. INVESTMENTS (Oct. 14, 2010), http://www.twinvestments.com/search?updated-max=2010-10-15T10%3A18%3A00%3A00-04%3A000&max-results=10 (“The electronic storage of information is a long-term growth story with exponential growth opportunities as more companies adopt online databases and the content itself dramatically increases in size . . . .”)
⁴ See Carmen Oveis Field, The Nuts and Bolts of Electronic Discovery—Technology Issues You Need to Know, N.J. LAW. MAG., Aug. 2007, at 10 (“The vast majority of one’s day-to-day communications in today’s ‘connected’ world is now handled electronically, with a blizzard of emails, text messages and instant messaging conversations largely replacing formal letters and telephone calls.”).
line media sources are becoming the go-to place for information.\(^5\) While the full costs and benefits of this social transformation have not been fully realized, the legal ramifications are already beginning to emerge.

An area that has been dramatically influenced by this social transformation is employment, specifically the impact of social media on the employee/employer relationship. In 2009, the Philadelphia Eagles football team suddenly terminated a part-time employee for making critical remarks about the team’s management on Facebook, a social networking website.\(^6\) Similarly, the Associated Press reprimanded a reporter for disparaging remarks posted on Facebook,\(^7\) and a North Carolina school district suspended a teacher due to comments she posted online regarding several students.\(^8\) These few examples illustrate a growing trend in the field of employment, one that is likely to continue.\(^9\)

Social media is widely used\(^10\) and acts as both a digital storage site\(^11\) and as a communication device.\(^12\) The popularity and the unique

---

\(^{5}\) See Matthew Mastromauro, Pre-Trial Prejudice 2.0: How YouTube Generated News Coverage is Set to Complicate the Concepts of Pre-Trial Prejudice Doctrine and Endanger Sixth Amendment Fair Trial Rights, 10 J. HIGH TECH. L. 289, 324 (2010) (“Due to the ease of public access, these Internet 2.0 websites also serve as some of the increasingly popular sources of media that make up the non-traditional news media, including blogs or other private websites that provide the average Internet user with his or her news, and have in recent years outpaced traditional news sources.”).

\(^{6}\) See Facebook Post Gets Worker Fired, ESPN.COM (Mar. 9, 2010), http://sports.espn.go.com/nfl/news/story?id=3965039 (“A Facebook post criticizing his employer, the Philadelphia Eagles, cost a stadium operations worker his job . . . . Dan Leone . . . was unhappy the team let Brian Dawkins sign with the Denver Broncos in free agency. According to the newspaper, Leone posted the following on his Facebook page: ‘Dan is [expletive] devastated about Dawkins signing with Denver . . . Dam Eagles Restarted [sic]!’”).

\(^{7}\) See Facebook Post Gets Worker Fired, ESPN.COM (Mar. 9, 2010), http://sports.espn.go.com/nfl/news/story?id=3965039 (“A Facebook post criticizing his employer, the Philadelphia Eagles, cost a stadium operations worker his job . . . . Dan Leone . . . was unhappy the team let Brian Dawkins sign with the Denver Broncos in free agency. According to the newspaper, Leone posted the following on his Facebook page: ‘Dan is [expletive] devastated about Dawkins signing with Denver . . . Dam Eagles Restarted [sic]!’”).


\(^{11}\) See generally Devjani Mishra, Seyfarth Shaw LLP, Web 2.0.10: Untangling the Risks of Electronic Social Media and Adapting Your Workplace Policies to Meet Them, in CORPORATE COUNSEL INSTITUTE 2010, at 47, 51 (PLI Corporate Law & Practice, Course Handbook Ser. No. B-1830, 2010) (reporting that in 2010 Facebook had over 400 million users who spent over 500 billion minutes on the site each month, including 50% of users who log in daily).

characteristics of social media websites, coupled with the general mis-
sunderstanding employees have regarding the scope of their legal
workplace protections, has caused this emerging technology to be-
come a major source of discomfort in employment relationships. As
a result, the use of social media has led to recent legal challenges by
both employees and employers. The courts have been slow to catch
up, as has often been the case with emerging technology, thereby
leaving employees and employers with little guidance on how and
when an employee’s Fourth Amendment privacy protection is trig-
gerated by the use of social media.

This Comment will attempt to define the scope of the privacy pro-
tection afforded to public employees through the Fourth Amend-
ment, as it would be applied to the information contained and
transmitted through social media websites. This Comment will focus
solely on the protection afforded to government employees through
the Fourth Amendment and how it might be applied to social media.
It will not touch on the very relevant issue of potential Fourth
Amendment implications based on information gathered from social
media sites or other Internet sources during the course of a criminal
investigation. Neither will this Comment cover private employees,

Facebook_rolls_out_storage_system_to_wrangle_massive_photo_stores (describing Face-
book’s new storage system, “Haystack,” developed in order to “better handle the growing
number of photos Facebook has to store”).

note_id=10150162289525301 (last visited Nov. 23, 2011) (“Facebook is designed to make
it easy for you to find and connect with others.”).

See generally Pauline T. Kim, Bargaining with Imperfect Information: A Study of Worker Percep-
tions of Legal Protection in an At-Will World, 83 CORNELL L. REV. 105, 110 (1997) (challeng-
ing the assumption that employees are sufficiently informed of their legal protections
based on the results of a survey in which “respondents overwhelmingly misunderstan[d]
the background legal rules governing the employment relationship”).

See Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *1, *6 (D.N.J.
Sept. 25, 2009) (upholding a jury verdict against defendant based on a violation of the
federal Stored Communications Act that resulted from the defendant-employer accessing
the plaintiff-employees’ social networking site); Bynorg v. SL Green Realty Corp., No. 05
Giv.0305 (WHP), slip op. at 1 (S.D.N.Y. Dec. 22, 2005) (denying defendant-employer’s
motion for preliminary injunction in a counterclaim suit against plaintiff-employee for
defamation based on statements posted on employee’s blog).

See Elizabeth Townsend Gard & Rachel Goda, The Fizzy Experiment: Second Life, Virtual
Property and a 1L Property Course, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 915, 927
(2008) (arguing that while other areas, such as business and education, continue to adapt, “courts and laws are notorious for being slow in catching up with new technolo-
gies,” leaving lawyers at a disadvantage by not being as familiar with growing industries).

See generally Nathan Petrashek, The Fourth Amendment and the Brave New World of Online So-
cial Networking, 93 MARQ. L. REV. 1495, 1496 (2010) (noting that both criminals and po-
lice are increasingly using social networking sites and arguing that the current Fourth
Amendment search doctrine in criminal cases fails to adequately protect user content).
as the Fourth Amendment’s privacy protection is not directly applicable to private employment relationships.\footnote{See Skinner v. Ry. Labor Executives’ Assoc., 489 U.S. 602, 623, 614 (1989) (holding that the Fourth Amendment does not apply to searches conducted by private employers, unless the private party acts as an instrument or agent of the Government).} Finally, this Comment will not touch on the many federal statutory claims that would be available, and which would have a far higher probability of success, to a public employee seeking relief based on an employer gaining access to information posted on social media websites.\footnote{There are a number of federal statutory claims an employee could bring based on unauthorized accesses by an employer or third party to information contained on a secure social media website. First, there is a possible violation of the federal Stored Communications Act, which makes it a crime (a) to gain unauthorized access to an electronic communication service provider’s facility, and (b) for a public electronic service provider to give up any communications held in electronic storage. See 18 U.S.C. §§ 2701–2702 (2006) (subjecting those who intentionally accesses, without authorization, or provides access to, the contents of electronic communication to penalties listed in 18 U.S.C. § 2701(b)). Second, the Wiretap Act makes it a crime to intercept a "wire, oral or electronic communication," which has been interpreted to include e-mail, unless the communication is readily accessible to the general public. 18 U.S.C. § 2511. These are merely a few sources of potential claims arising out of this sort of employment situation.} Rather, the focus here is on a federal constitutional claim based on a violation of the implicit right to privacy in the Fourth Amendment.

Despite the limited scope, this analysis is still relevant for several reasons beyond its direct application to the over twenty-three million federal, state, and local employees who would be eligible to bring a federal claim based on the Fourth Amendment.\footnote{See id. at 292 (explaining how the tort of “intrusion upon seclusion” is the most widely recognized common-law privacy claim in the employment context and that such a claim hinges primarily on whether the intrusion was into an area where the employee had a reasonable expectation of privacy).} First, many of the concepts contained in the Court’s Fourth Amendment analysis are analogous to those found in many tort-based protections that govern the private employment relationship.\footnote{See Privacy Protections in State Constitutions, NAT’L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13467 (last visited Nov. 24, 2011) (listing all the states with an explicit constitutional right to privacy). See generally ALASKA CONST. art. I, § 22 (“The right of the people to privacy is recognized and shall not be infringed.”); MONT. CONST. art. II, § 10 (“The right of individual privacy is essential to the well-being of the individual.”).} The way the Court analyzes the expectation of privacy in the context of online information will, therefore, likely be considered in private tort claims against employers. Second, a federal recognition of the right to privacy in social media would have a reverberating impact on the application of state constitution privacy protections. Many states, unlike the federal constitution, explicitly provide a right to privacy.\footnote{See Privacy Protections in State Constitutions, NAT’L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13467 (last visited Nov. 24, 2011) (listing all the states with an explicit constitutional right to privacy). See generally ALASKA CONST. art. I, § 22 (“The right of the people to privacy is recognized and shall not be infringed.”); MONT. CONST. art. II, § 10 (“The right of individual privacy is essential to the well-being of the individual.”).} So far these state
rights of privacy have rarely been applied, if at all, to electronic and
Internet usage. Courts in some of the states with an explicit right of
privacy look to federal interpretation of constitutional privacy protec-
tion for “authoritative guidance on the meaning of the state constitu-
tion.” Thus, if and how the Court applies the Fourth Amendment
to social media use by employees would likely impact whether similar
claims are brought under state privacy laws, as well as how courts
would respond to such claims.

The analysis will be broken down into three main sections. In the
first section I will set up the issue by providing background on the
Fourth Amendment’s application to employees. Part I will detail the
background of the Fourth Amendment and the concerns that gave
rise to the current standard developed for assessing Fourth Amend-
ment privacy protection in the public workplace. Part II will give a
brief overview of social media in its various forms, as well as classify
the different variations of social media into generalized categories
that are more workable for doctrinal purposes. Part III will detail
some of the legitimate concerns of employers that are implicated by
an employee’s use of social media, and the methods by which em-
ployers are able to monitor such use. Finally, Part IV will lay out the
Court’s current approach to employee privacy claims under the
Fourth Amendment.

In the second section I will explain how the Fourth Amendment
likely does not protect social media use by employees. Part V argues
that under the Court’s current Fourth Amendment framework, an
employer’s surveillance of an employee’s social media use would not
be a violation for three reasons. First, the Court would most likely
hold that employees have no expectation of privacy in social media
use because it inherently involves disclosure to third parties. Second,
even if the Court were to disregard this implicit waiver of privacy, so-
cial media use would still fall outside Fourth Amendment protection
based on the Court’s use of physical and spatial boundaries for de-
termining whether an employee has an expectation of privacy. Fin-
ally, if the Court were to grant the employee a reasonable expecta-

\[\text{\begin{quote}
\text{of a free society and shall not be infringed without the showing of a compelling state in-
terest.}\)
\end{quote}\]

\[\text{22 See Rustad & Paulson, supra note 2, at 842 ("[T]o date, no court has extended state con-
stitutional rights of privacy to e-mail monitoring or electronic surveillance.").}\]

Rev. 215, 217 (1989).}\]

of privacy based on the context of the employment relation, specifically the frequency or
need of an employer to access the employee’s workspace).}\]
tion of privacy, the Court’s most recent decision regarding the scope of employee privacy protection appears to advance the growing trend in Fourth Amendment analysis of giving greater deference to the employer in balancing the reasonableness of the expectation against the legitimate interests of the employer.

Finally, in the third section I will argue that despite these obstacles, the Court should extend Fourth Amendment protection to this new technology because there is an expectation of privacy in social media use in the employment context and because that expectation can be sufficient to override a legitimate governmental interest. My justification for why social media use should be covered by the Fourth Amendment is based on the prevalence of social media use, its transformation into a means of storing information as opposed to just being used to share information, and the general (and growing) assumption that such use is private. That protection, however, should not be without limits. The courts must recognize the unique characteristics of social media and determine a method of evaluating when a reasonable expectation should be applied to this new technology. I contend that such an evaluation must take into consideration the scope of the audience and the method by which the users attempt to secure the information. Therefore, the Fourth Amendment should protect social media use by public employees if the employee takes reasonable measures intended to restrict access to their online information.

I. BACKGROUND ON THE FOURTH AMENDMENT

"The basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."

The Fourth Amendment protects individuals from “unreasonable searches and seizures” by government agents absent “probable

25 See City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010) (regarding an adverse employment action taken as a result of a review by the government employer of text messages sent by a city employee).

26 See Michelle Hess, Note, What’s Left of the Fourth Amendment in the Workplace: Is the Standard of Reasonable Suspicion Sufficiently Protecting Your Rights, 15 Fed. CIR. B.J. 255, 277 (2005) (“Unfortunately, the Fourth Amendment rights of employees have been almost completely eviscerated over time with the explicit sanction of the judicial branch.”).

Traditionally, this was interpreted as only protecting against a government intrusion of an individual’s property interest. That protection eventually expanded to cover an overarching “expectation of privacy,” which some argue had always been the underlying and implicit concept of the Fourth Amendment. In Katz v. United States, the Court expanded the Fourth Amendment's protection beyond mere physical intrusions based on the reasoning that the amendment protects “people—and not simply ‘areas’—against unreasonable searches and seizures.” That decision is, rightly or wrongly, widely considered precedent for the proposition that the “expectation of privacy” is the main objective of the Fourth Amendment’s protection.

In broadening the scope of Fourth Amendment protection beyond a simple property based analysis, the Court created more ambiguity as to when the protection applies. Before Katz, courts applied the legal standards developed for determining property interests when distinguishing between a valid and an invalid seizure. In the wake of Katz, courts were suddenly required to make determinations as to when a reasonable person would have a legitimate expectation of privacy. The only guidance offered by the Court as to determining when a reasonable expectation of privacy exists was a two step in-

28 U.S. CONST. amend. IV.
29 See Ricardo J. Bascuas, Property and Probable Cause: The Fourth Amendment’s Principled Protection of Privacy, 60 RUTGERS L. REV. 575, 580 (2008) (noting that, prior to 1967, the Fourth Amendment was only applied to violations of a property interest and that the “‘[e]xpectations of privacy’ are a legal fiction of relatively recent invention”).
30 See id. at 584–85 (arguing that prior to 1967 the concept of privacy had always been central to Fourth Amendment analysis, but that the Court assumed that interest was sufficiently protected by an explicit protection of property).
32 See Bascuas, supra note 29, at 584 (recognizing that the Katz decision is interpreted as solidifying the proposition that the Fourth Amendment guarantees a right to privacy).
33 See id. at 580–81 (noting that prior to 1967, violations of “property interests” were construed using their legal definitions). See, e.g., Silverman v. United States, 365 U.S. 505, 509 (1961) (deciding not to reconsider the Court’s previous decisions which held that a physical intrusion is necessary in order to claim a Fourth Amendment violation because "a fair reading of the record in this case shows that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by the petitioners"); Goldman v. United States, 316 U.S. 129, 135 (1942) (holding “that the use of the detectaphone by Government agents was not a violation of the Fourth Amendment”); Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that a police wiretap on the defendant’s phone did not violate the Fourth Amendment violation because such a violation cannot occur “unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house”).
34 See Bascuas, supra note 29, at 580 (arguing that “expectations of privacy” are subjective specters that, like shapes in the clouds, judges view idiosyncratically).
quiry that looked first at the individual’s subjective expectation and, second, whether that expectation was “one that society is prepared to recognize as reasonable.” The obvious problem with shifting from a concrete property analysis to an abstract privacy analysis is that “[p]rivacy is an extremely broad concept.” And, unfortunately, the Court in *Katz* offered little specificity as to what a reasonable expectation would entail. The shift ultimately ensured that the Court would have to continually revisit the Fourth Amendment’s application in order to make it adaptable to the changes in society’s expectations.

The Fourth Amendment is commonly asserted in the criminal context when defendants challenge the admissibility of evidence based on the process through which it was acquired. The Court, however, has interpreted the Amendment as applicable to public employees as well, thereby extending the Amendment’s protection to cover intrusions by the government in its capacity as an employer. As the Court reasoned, “it would be ‘anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.’” The scope of the protection afforded by the Fourth Amendment, however, is different depending on whether it is being applied to a criminal defendant or a public employee. Thus, while it is well

---

35 *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also* Haley Plourde-Cole, *Back to Katz: Reasonable Expectation of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571, 580 (2010) (noting that Justice Harlan’s interpretation of the majority opinion is that a reasonable expectation of privacy is established by the subjective expectation of the individual, as well as the overall expectations of society).


37 *See* Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1312 (2002) (“In the end, both the majority opinion [in *Katz*] and Harlan’s explanation of the phrase ‘reasonable expectation of privacy’ were sufficiently meager that the task inevitably fell to future courts to define the phrase more fully.”).

38 *See* Olmstead, 277 U.S. at 465–66 (citing many cases that indicate a Fourth Amendment violation will occur when a criminal defendant has his “papers or his tangible material effects” seized by the government).

39 *See* O’Connor v. Ortega, 480 U.S. 709, 714 (1987) (“The strictures of the Fourth Amendment, applied to the States through the Fourteenth Amendment, have been applied to the conduct of governmental officials in various civil activities.”); *see also* Nat’l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 665 (1989) (recognizing that the Fourth Amendment “protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer”).


41 The Fourth Amendment in the criminal context has what are known as the “warrant requirement” and the “probable cause requirement,” neither of which are necessarily applicable to the Government in its role as an employer. *See* Skinner v. Ry. Executives’ Assoc., 489 U.S. 602, 623 (1989) (holding that the warrant requirement of the
settled that the Fourth Amendment’s privacy protection extends to public employees, that protection is limited by the legitimate needs of public employers to monitor employees and ensure a safe and efficient working environment.\textsuperscript{42}

II. THE VARIOUS FORMS OF SOCIAL MEDIA

“We lived in farms then we lived in cities and now we’re gonna live on the internet.”\textsuperscript{43}

There are many new web-based technologies, in addition to social media, that are creating new and interesting problems for employers.\textsuperscript{44} Social media, however, presents a unique problem for Fourth Amendment analysis and emphasizes the shortcomings of the current judicial understanding of the Internet in the context of the Fourth Amendment. Unlike e-mail, instant messaging, or even Internet search history, social media necessarily has an additional public aspect to it because it is shared with a broader range of individuals, as opposed to a single recipient. This presents a more difficult question regarding privacy because there is inherently some diminished expectation of privacy, and because it cannot as easily be analogized to older forms of technology.\textsuperscript{45} It is, therefore, important to distinguish...
social media from other forms of web technology in order to properly understand why it is going to become a hotbed of employment litigation, and how it needs to be specifically addressed by the Court in order to properly be squared with the current Fourth Amendment framework.

A social media site typically incorporates one or more of the following: blogs, microblogs (Twitter), social networks (Facebook, MySpace, LinkedIn), media sharing (YouTube), wikis, and virtual worlds. The main difference between these elements of social media and other web based technologies, such as electronic communication (like e-mail and instant messaging) and online storage (like Mozy), is the sharing aspect. All of the previously listed types of social media, to varying degrees, intend that the information be shared with other people besides an intended recipient. In most cases, unlike e-mail and text messaging, the information does not have an intended receiver; rather it is posted for viewing by a group whose

46 “Blogs—Web logs or journals, in which site authors and users can post textual, audio or video content and, in many cases, comment on others’ blog posts.” Mishra, supra note 10, at 50.

47 “Microblogs—Sites and spaces allowing users to post short blog entries (usually 160 characters or less).” Id.

48 “Social Networks—Sites at which users create customized profiles and form connections with other users based upon shared characteristics and interests . . .” Id.; see also Petrashek, supra note 16, at 1500–01 (“An online social network can therefore be defined as an online service that encourages self-disclosure by requiring members to populate a profile with personal information and allows them to create a virtual community by linking their personal profile with those of other members.”).

49 “Media Sharing—Sites to which users post and share videos, audio files and/or photos as well as tag them to enable searchability.” Mishra, supra note 10, at 50.

50 “Wikis—Resources or documents edited collaboratively by a community of users with varying levels of editorial control by the website publisher.” Id.

51 “Virtual Worlds—Web or software-based platforms that allow users to create avatars or representations of themselves, and through these avatars to meet, socialize and transact with other users.” Id.

52 “Instant messaging is the exchange of text messages in real time between two or more people logged into a particular instant messaging (IM) service. Instant messaging is more interactive than e-mail because messages are sent immediately, whereas e-mail messages can be queued up in a mail server for seconds or minutes.” Steven Goode, The Admissibility of Electronic Evidence, 29 Rev. Litig. 1, 16 n.64 (2009) (quoting Definition of: Instant Messaging, PCMag.COM, http://www.pcmag.com/encyclopedia/ (search “instant messaging”) (last visited Sept. 20, 2010)).

53 Mozy is one of the leading companies that provides online backup service. Users automatically transmit data from their personal or work computers to a secure database maintained by Mozy and then are able to retrieve that information if their computer is damaged or information is lost. See About Mozy, MOZY, http://mozy.com/about (last visited Nov. 23, 2011).
members may or may not have been limited by the original poster.\textsuperscript{54} Due to this unique feature, the exclusivity of the audience is paramount in assessing an individual’s reasonable expectation of privacy in social media use, and that exclusivity is dependent on the various security features offered by different social media sites.

Even after assessing the form of the social media in question, no legal analysis of social media is complete without evaluating the security features employed by the user. The security features of social media sites should be a central component to any inquiry into determining the applicability of the Fourth Amendment to this technology. The security technology varies from site to site, even from user to user within a single site, and with it so too does the reasonableness of the user’s expectation of privacy. Some sites may require viewers to have a password (presumably provided by the author of the content) to access the site where the information is posted.\textsuperscript{55} Other sites allow authors to select, either individually or as a group, viewers who will be able to see the information disseminated on the social media site.\textsuperscript{56} Finally, another way users attempt to protect their privacy is through the use of pseudonyms and avatars, which attempt to shield the identity of the user from whoever views the content.\textsuperscript{57}

\textsuperscript{54} On Facebook and Twitter users can make “status updates” or “tweets,” which can then be viewed by other users. A user can limit who has access to their “status updates” or “tweets” by altering their security settings. See Petrashek, supra note 16, at 1507 (“Facebook offers users an advanced series of privacy settings to restrict others’ ability to access their profile content. Users can control the visibility of nearly all the information shared through Facebook, including their . . . status updates and comments.”).

\textsuperscript{55} See Wendi S. Lazar et al., Outten & Golden LLP, Do Employees Have Privacy Rights in the Digital Age?, in EMPLOYMENT DISCRIMINATION LAW AND LITIGATION 2010, at 217, 228 (PLI Litig. & Admin. Practice, Course Handbook Ser. No. H-828, 2010) (warning that an employer’s technology policy may not negate privacy violations, especially when it involves “restricted-access social networking site profiles or password-protected blogs”).

\textsuperscript{56} See Data Use Policy, FACEBOOK, http://www.facebook.com/about/privacy/your-info#howweuse (last visited Nov. 29, 2011) (“While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don’t share information we receive about you with others unless we have: . . . received your permission; . . . given you notice, such as by telling you about it in this policy; or . . . removed your name or any other personally identifying information from it.”).

\textsuperscript{57} Pseudonyms are most commonly used on the Internet to create user identifications for the purchase and sale of items, but they are also used to shield the user from being identified. See Bert-Jaap Koop et al., Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 11 MINN. J. L. SCI. & TECH. 497, 502 (2010) (“In some situations, the pseudonym is used to conceal the true identity of the person, acting as a privacy-enhancing tool. Pseudonyms also function as user IDs in the information society. On the Internet, many people use a pseudonym (or multiple pseudonyms) to stay anonymous.”). On the other hand, avatars are intended to be representations of the user within the context of online games and virtual realities. Those representations, however, can them-
These varying degrees of security impact the reasonableness of the expectation of privacy one has in the information provided through social media. If the Court were eventually willing to extend Fourth Amendment protection to social media use, it would have to consider these security features in determining the extent to which an employee has a reasonable expectation of privacy. While most of these social media sites are making it easier to limit who has access to the user’s information, a user could fail to take advantage of these measures, thereby opening up their online profile to anyone with a computer.

In order to keep track of the variety of forms that electronic communication and social media can take, it is helpful to create generalized categories in which to classify those forms. For the purposes of this Comment, I will create three categories of electronic communication and social media in order to help analyze how the Fourth Amendment applies to them. The first category, which I will call “Level I,” consists of all electronic storage and direct communication. This category includes any electronic transformation of information that is either intended to be stored, meaning it is not intended to be viewed by anyone, or any information intended to be sent to a single recipient or class of recipient (e-mails, instant messaging, Facebook messages). “Level II” will include any electronically transmitted information that is intended to be viewed by a pre-selected group. This is what I will call the “limited sharing of information” and includes such things as Facebook “posts,” any “profile” information that is visible only to a certain class of individuals predetermined by the content author, or any password-protected blogs. Finally, “Level III” involves what I call “unlimited sharing of information,” whereby the content author disseminates information online that is available to anyone who has access to the social media site. For example, a Tweet, Wikipedia post or comment posted on a third party website would fall in this last category. Ultimately, there are many variations on the many forms social media can take, and it is difficult to make legal determinations on broad generalizations. These categories, however, are

58 Note that Level II classification will often depend on the security measures taken by the users, so it is possible for the same type of social media outlet to be both Level II and Level III, depending on the user.
useful because they are based on some of the underlying principles, such as disclosure and access, which are important in a Fourth Amendment analysis.

III. LEGITIMATE INTEREST OF GOVERNMENT EMPLOYERS

"By releasing stolen and classified documents, WikiLeaks has put at risk not only the cause of human rights but also the lives and work of these individuals."

The increased use of social media creates many concerns for employers and provides legitimate reasons for wanting to monitor more closely the content distributed by their employees onto such sites. Coupled with a growing ability to be successful in monitoring electronic use by an employee, there is no doubt that this issue has and will continue to create a lingering tension between employers and employees. These concerns are important because even if there is an expectation of privacy in social media use, there is still a possibility that an employee’s Fourth Amendment rights could be superseded by the legitimate needs of the government employer who accesses the information in a reasonable way. This Part addresses what those needs might be and what ways an employer can and does monitor its employees’ use of electronic information sharing.

A major concern for government employers is the potential to be held liable for the use of social media by their employees. Co-worker harassment represents one potential area of liability, whereby “[a]n employer is liable for co-worker harassment if it knew or reasonably should have known about the harassment and fails to take appropriate remedial action.” Thus, if an employer who has access to an employee’s online social media forum, and through that access has the ability to witness “harassing comments or offensive dialogue being exchanged among employees and does nothing, the employer may later be accused of having knowledge of co-worker harassment and failing to respond.” The employer may not even have actual knowledge of the harassing conduct; the access alone may be enough to bring a claim. Indeed, this form of liability has already been ac-

---


61 Id. at 18.
ceived as a plausible cause of action and, therefore, electronic harassment between co-workers is a legitimate concern.\textsuperscript{62}

Another way employee social media use puts an employer risk due is in a defamation suit. An employer is liable for the actions of an employee if the employee harms someone while acting in the scope of their employment.\textsuperscript{63} If an employee writes defamatory remarks regarding someone in their role as an employee, such as a customer, the employer could be liable.\textsuperscript{64} These concerns are legitimate because they directly affect the financial stability of the employer as well as other employer interests. There are also a slew of less direct employer concerns based on social media use, including: the loss of trade secrets,\textsuperscript{65} workplace productivity,\textsuperscript{66} and reputation of the employer.\textsuperscript{67}

\begin{footnotesize}
\begin{enumerate}
\item See Blakey v. Cont’l Airlines, Inc., 751 A.2d 538, 543 (N.J. 2000) (reversing a motion to dismiss in favor of defendant company who failed to take action in response to harassing comments made on a company electronic bulletin board by an employee against another employee because, “[a]lthough the electronic bulletin board may not have a physical location within a terminal, hangar or aircraft, it may nonetheless have been so closely related to the workplace environment and beneficial to Continental that a continuation of harassment on the forum should be regarded as part of the workplace”).
\item The common law doctrine of respondeat superior holds that an employer may be liable for the actions of an employee if those actions take place within the scope of employment. See 27 AM. JUR. 2D Emp’l Relationship § 373 (2010) (“Under the theory of respondeat superior, an employer can be held vicariously liable for an employee’s tortious act against the person or property of a third party in the transaction of the employer’s business. Respondeat superior liability extends to cases where the risk was one that may fairly be regarded as typical of or broadly incidental to the enterprise undertaken by the employer.”).
\item See Krinsky v. Doe, 72 Cal. Rptr. 3d. 231, 234 (Cal. App. 2008) (protecting the identity of the pseudonymous posters who contributed to a conversation on a financial message board that “devolved into scathing verbal attacks on the corporate officers of a Florida company, prompting a lawsuit by one of those officers”).
\item An employer always has an interest in making sure its employees are not divulging trade secrets because such conduct can be detrimental to the business. This concern is heightened with the emergence of social media because users have begun to provide substantial details about their daily activities, and by doing so, may unknowingly express information (such as scheduling, rotations, etc.) that is confidential.
\item Workplace productivity may be one of the biggest concerns for an employer, but it is hard to say whether it is indeed legitimate for the purposes of Fourth Amendment analysis. While employees do spend an enormous amount of time on these sites, the concern is not about the information being disseminated, rather it is the very act of being online that is causing detriment to the employer. See Renee M. Jackson, Social Media: Counsel for Clients and Firm Managers, LAW OFF. MGMT. & ADMIN. REP. (Apr. 2010), at 1, 14 (“The most obvious hazard regarding the use of social media during employment is internal to the organization: Employees may spend so much time using social media during working hours that productivity decreases.”); see also Ryann MacDonald & Brendan Kroepsch, Workplace Privacy: The Social, Technical, and Ethical Ramifications, in TECHNOLOGY AND PRIVACY IN THE NEW MILLENNIUM 137 (Kai Larsen & Z. Voronovich eds., 2004) (noting
\end{enumerate}
\end{footnotesize}
Finally, certain public employment positions create an even greater interest in monitoring employee conduct based on the sensitive nature of information the employee has access to. As exemplified by the recent WikiLeaks controversy, whereby a social media site published thousands of classified government documents, governmental employers clearly have a legitimate interest in monitoring the social media use of their employees in order to ensure confidential governmental information is not distributed unlawfully. The ramifications for failing to adequately monitor employees in this context could range from mere public embarrassment to putting lives at risk. Thus, no matter how extensive an employee’s expectation of privacy, it should be noted that in certain situations the needs of the employer would take priority.

Employers’ legitimate concerns led to new and innovative ways of monitoring workers. As employees have benefited from the rise in technology, so too have employers benefited from new methods of electronic surveillance. Thus, due to the many legal and financial repercussions that can result from an employee’s use of social media, many employers have made it their practice to monitor such action. Before, during and even after employment, employers check up on their employees to make sure that they do not harm the company.

---

67 That “62% of employees admitted to using the Internet for personal use on a daily basis, and 44% use their company e-mail account for both work and personal use”).

68 The reputation of the employer is at a far greater risk since the emergence of social media sites. In some cases, the employee may not even be aware that his or her use of the sites is generating a negative image of his or her employer. For example, Facebook has what is known as “community pages” which are general sites dedicated to certain topics (or businesses) developed based on information provided in personal profiles. See Kashmir Hill, Law Firm Facebook Pages Reveal How Associates Really Feel (June 1, 2010, 3:05 PM), http://abovethelaw.com/2010/06/law-firm-facebook-pages-reveal-how-associates-really-feel.


70 See Adam Levine, Rights Groups Express Concerns About WikiLeaks, CNN (Aug. 10, 2010), http://articles.cnn.com/2010-08-10/us/wikileaks.rights.groups_1_wikileaks-julian-assange-rights-groups?_s=PM:US (describing how some activist groups have expressed concerns that the information contained in some of the documents released by WikiLeaks would put specific Afghanistan citizens in danger of being targeted by the Taliban for helping Western troops).
But even beyond preventing harm to the company, employers utilize this method of surveillance to evaluate whether or not an individual should be hired or remain employed. One of the main areas that employers make use of social media monitoring is in pre-employment screening.\footnote{With so many factual inaccuracies provided by job applicants, and with potential exposure to liability based on employee conduct, employers turn to social media as an additional tool to perform background checks on potential employees. See Michael Jones et al., The Ethics of Pre-Employment Screening Through the Use of the Internet, in THE ETHICAL IMPERATIVE IN THE CONTEXT OF EVOLVING TECHNOLOGIES 43–44 (Dan McIntosh et al. eds., 2004) (noting that nearly 50% of resumes contain factual errors, which in turn has led to “[a] growing trend in the business world today . . . to use internet search engines and social networking sites to screen job applicants,” specifically citing a survey indicating that “26% of hiring managers have used internet search engines to research prospective employees, while 12% say they have used social networking sites”). Recently, the Court unanimously held that while potential government employees do have a privacy interest, that interest is subservient to the government’s need to perform background checks. See NASA v. Nelson, 131 S. Ct. 746, 758 (2011) (“As this long history suggests, the Government has an interest in conducting basic employment background checks. Reasonable investigations of applicants and employees aid the Government in ensuring the security of its facilities and in employing a competent, reliable workforce . . . . We hold . . . that, whatever the scope of this [privacy] interest, it does not prevent the Government from asking reasonable questions . . . in an employment background investigation.”).} Employers also monitor employees’ electronic communication during the course of employment by using “flagging” software.\footnote{Matthew E. Swaya & Stacey R. Eisenstein, Emerging Technology in the Workplace, 21 LAB. L. 1, 9 (2005).} This software screens an employee’s electronic communications, such as e-mails, for certain words or phrases and then sends these flagged messages to an employer representative.\footnote{Id.} Several government agencies are using flagging software and it is likely to become only more prevalent in public workplaces.\footnote{See id. (“Both the Department of Justice and the Department of Energy, for example, reportedly installed software that censored employee e-mails containing inappropriate language.”).} A second important monitoring device utilized by employers is “keystroke logging,” whereby an employer can track what a specific employee views, and even go so far as logging every single keystroke.\footnote{See id. (“Some keystroke logging devices record the identity of employees who access employer databases and can track what the employees viewed. Other keystroke logging devices are more precise, logging every key touched by a particular employee, and saving that information on a separate server.”).} This technology can be valuable for monitoring social media because social media websites often require user passwords in order to view the content. Keystroke logging would provide employers the ability to obtain such passwords if the employee accessed the site using an employer’s com-
A question might be raised as to the reasonableness of the method of using these devices; however, courts would most likely consider such methods permissible.

This Part was intended to illustrate that not only do employers have legitimate interests in monitoring an employee’s use of social media, but that they also have the capability to do so. Any Fourth Amendment analysis into an employee’s privacy protection must involve a balance of the employer’s interests and an evaluation as to the method by which the employer obtains the information.

IV. THE CURRENT FOURTH AMENDMENT FRAMEWORK FOR EMPLOYEE PRIVACY CLAIMS

“The American society with which I am familiar ‘chooses to dwell in reasonable security and freedom from surveillance . . . .’

The current Fourth Amendment analysis in the employment context, and the one reaffirmed in City of Ontario v. Quon, comes from O’Connor v. Ortega. In O’Connor, the Court held that public employees can have Fourth Amendment privacy protection in the workplace, depending on the reasonableness of the expectation of

---

76 It should be noted that employees may retain an expectation of privacy even as to information stored on an employer-owned computer hard drive, depending on the expressed expectation policies of the employer. See Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (noting that there could be a right to privacy in employer-owned equipment provided to employees so long as the employer has not destroyed any expectation of privacy by declaring a policy of inspecting the equipment). However, here we are talking not about locally stored files, but rather virtually stored passwords to information.

77 These methods of monitoring employees are analogous to global positioning satellite (“GPS”) tracking devices that employers put on company vehicles. Furthermore, “courts that have considered the issue have concluded that an employer may install a GPS device in an employer-owned vehicle.” Kendra Rosenberg, Location Surveillance by GPS: Balancing an Employer’s Business Interest with Employee Privacy, 6 WASH. J. L. TECH. & ARTS 143, 152 (2010). Therefore, most likely these other monitoring practices would not be successfully challenged so far as the method of gathering the information is concerned. It is possible, however, that a distinction could be drawn from these types of cases by the value of the asset that the employer is monitoring. Courts might be more inclined to accept employer-monitoring practices if they center on an employer-owned asset, such as a company computer’s hard drive, as opposed to monitoring information contained on a third party server.


79 See City of Ontario v. Quon, 130 S. Ct. 2619, 2628–29 (2010) (explaining that the case can be decided without clarifying the two approaches taken in O’Connor because both the plurality and Justice Scalia’s opinion would lead to the same result based on the facts of the case).
privacy. The Court set up a two-part analysis for courts to use in assessing Fourth Amendment workplace privacy claims and for determining whether an employee’s constitutional rights were violated.

The first part of the test looks to see whether the employee had a reasonable expectation of privacy in the area intruded on by the employer or in the object of the search. The O’Connor opinion offered two distinct approaches for this initial inquiry. The Quon decision, however, failed to clarify which standard is the appropriate one because it determined that under either standard the plaintiff had an expectation of privacy. Therefore, the question as to which standard applies remains open.

The plurality sets up an “operational realities” framework for analyzing the reasonableness of the expectation. Under this standard reasonableness is extremely contextual and determined on a case-by-case basis taking into consideration the work environment and the employment relationship. Justice Scalia concurred that an employee could have a reasonable expectation of privacy, but disagreed with the plurality’s “operational realities” approach to assessing that expectation largely because it left an “open invitation for employers to regulate privacy out of existence by manipulating the context of the workplace.”

---

80 See O’Connor v. Ortega, 480 U.S. 709, 717 (1987) (rejecting the argument that “public employees can never have a reasonable expectation of privacy in their place of work”); see also Justin Conforti, Somebody’s Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit’s Misapplication of the Ortega Test in Quon v. Arch Wireless, 5 SETON HALL CIR. REV. 461, 472–73 (2009) (“[T]he Supreme Court announced that public-sector employees may enjoy some privacy in the physical workplace, such as desks and file cabinets, based on whether the context of a particular workplace fosters within the employee a reasonable expectation of privacy.”).

81 See O’Connor, 480 U.S. at 719 (deciding first that the employee had a reasonable expectation of privacy before looking at whether the search was reasonable); see also Conforti, supra note 80, at 473 (“To guide lower courts in investigating Fourth Amendment workplace privacy claims, the plurality applied a two-part inquiry.”).

82 See O’Connor, 480 U.S. at 715 (noting that Fourth Amendment rights are only implicated if the conduct “infringed ‘an expectation of privacy that society is prepared to consider reasonable’”) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

83 See Quon, 130 S. Ct. at 2634 (Stevens, J., concurring) (noting that the majority failed to resolve whether the plurality opinion in O’Connor is controlling).

84 See O’Connor, 480 U.S. at 717 (noting that while employees do not lose their Fourth Amendment rights “merely because they work for the government . . . [t]he operational realities of the workplace, however, may make some employees’ expectations of privacy unreasonable”).

85 Id. at 718.

86 O’Connor, 480 U.S. at 731 (Scalia, J., concurring); Conforti, supra note 80, at 474.
public employees have a reasonable expectation of privacy as to the contents of their offices.\(^87\)

If there is a reasonable expectation of privacy, then the Court looks to see whether the employer’s intrusion was reasonably justified.\(^88\) According to the plurality, determining whether or not a search was reasonable requires balancing the nature of the intrusion against governmental needs.\(^89\) This balancing test must be applied in two stages: first it must be applied to the justification for the search; and second, it must be applied as to the conduct of the search.\(^90\) Thus, when conducted for a non-investigatory, work-related purpose or for the investigation of work-related misconduct, a government employer’s search is reasonable if it is justified at its inception and if the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search.\(^91\)

V. SOCIAL MEDIA UNDER THE CURRENT FRAMEWORK

“The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The 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.”\(^92\)

As it stands now, the current framework of workplace privacy protection under the Fourth Amendment would likely not cover social media use. First, social media use would not be given the expectation

---

\(^{87}\) O’Connor, 480 U.S. at 731 (Scalia, J., concurring).

\(^{88}\) Id. at 719; see also Conforti, supra note 80, at 479 (“The reasonableness of an employer’s search has two components. First, the search must be reasonable at its inception, with the employer having some ‘reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct.’ Second, the search must be reasonable in scope, which requires the employer to adopt measures that are ‘reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct].’” (quoting O’Connor, 480 U.S. at 725–26)).

\(^{89}\) See O’Connor, 480 U.S. at 719 (“A determination of the standard of reasonableness applicable to a particular class of searches requires ‘balanc[ing] the nature and quality of the intrusion on the individual’s Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.’” (quoting United States v. Place, 462 U.S. 696, 703 (1983))).

\(^{90}\) Conforti, supra note 80, at 479.

\(^{91}\) O’Connor, 480 U.S. at 725.

\(^{92}\) Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) (holding that searching an employee’s text messages was reasonable and was not an infringement of Fourth Amendment rights), rev’d sub nom. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
of privacy because of the Third Party Doctrine.\textsuperscript{93} Second, even if social media use were exempted from the Third Party Doctrine, a straightforward application of either test offered by the Court in \textit{O'Connor} would likely result in the conclusion that no reasonable expectation of privacy exists in most types of social media use. Finally, even if the Court did find a reasonable expectation of privacy, it will be difficult for any claim against an employer to pass the Fourth Amendment balancing test because the Court gives great deference to the employer if notice regarding the potential for electronic monitoring is provided.

A. Waiver of Privacy

The reason social media presents a unique problem for Fourth Amendment analysis is because of the historical Third Party Doctrine, which assumes a privacy expectation is destroyed once disclosure is made to a third party.\textsuperscript{94} This exception was originally acknowledged in \textit{Katz},\textsuperscript{95} but was subsequently put into practice in \textit{United States v. Miller}, where the Court held that bank records were not subject to Fourth Amendment protection because they were not in the individual’s possession.\textsuperscript{96} Ultimately, the Third Party Doctrine has come to hold that one “has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”\textsuperscript{97}

Social media could be considered to have three stages of third party disclosure. The first stage of disclosure is made to the Internet Service Provider (“ISP”), which acts as the conduit through which the

\textsuperscript{93} The Third Party Doctrine states that an individual’s expectation of privacy is destroyed when he or she discloses the information to a third party. \textit{See} Orin S. Kerr, \textit{The Case for the Third Party Doctrine}, 107 Mich. L. Rev. 561, 563 (2008) (“By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed. . . . ‘In other words, a person cannot have a reasonable expectation of privacy in information disclosed to a third party.’” (quoting \textit{Katz} v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))).

\textsuperscript{94} \textit{See} Petrashek, \textit{supra} note 16, at 1519 (noting that under the current search doctrine, voluntary disclosure to third parties can destroy one’s privacy expectations in shared non-content information).

\textsuperscript{95} \textit{See Katz}, 389 U.S. at 351 (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”).

\textsuperscript{96} \textit{United States v. Miller}, 425 U.S. 435, 443 (1976) (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Governmental authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

\textsuperscript{97} \textit{Smith v. Maryland}, 422 U.S. 735, 743 (1979).
information travels to its destination. This type of third party disclosure is similar to the way a telephone provider or post office acts as a third party to phone conversations or letters. Due to the similarity, a court has already applied the Fourth Amendment to content information sent through an ISP in the same way it has to the information sent through telephone providers and post offices. As with telephone calls and letters, however, non-content information, such as the subscriber information (i.e. who sent/received the phone call/letter) is not protected.

In the second stage, social media websites, as with electronic storage websites, are maintained by a specific entity, such as Facebook, which stores much of the information disseminated through the site on its third party servers. Whether or not this would be considered a third party disclosure is unclear because the Court has yet to apply the Third Party Doctrine to the Internet. The only guidance from the Court stems from its content/non-content distinction developed in Smith v. Maryland, and that has little applicability to the Inter-

---

98 See Internet Service Provider (ISP), Britannica Academic Edition, available at http://www.britannica.com (search “internet service provider”) (last visited Nov. 23, 2011) (“[C]ompany that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet, ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page. ISPs can host Web sites for businesses and can also build the Web sites themselves. ISPs are all connected to each other through network access points, public network facilities on the Internet backbone.”).

99 See United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (“Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection . . . . If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment.”); see also Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 Mercer L. Rev. 507, 527–28 (2005) (“[A]s with postal mail and telephone conversations, the sender of e-mail retains no REP [reasonable expectation of privacy] in the addressing components, but should retain a REP in the contents.”).

100 See United States v. Perrine, 518 F.3d 1196, 1294 (10th Cir. 2008) (“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”); see also United States v. Forrester, 512 F.3d 500, 504, 511 (9th Cir. 2008) (holding that e-mail to/from addresses and IP addresses constitute addressing information and are therefore not considered "searches" for Fourth Amendment purposes).

101 Petrashek, supra note 16, at 1520.

102 See Smith, 442 U.S. at 743 (drawing a distinction between the contents of a telephone call and the number dialed, the former being protected by the Fourth Amendment and the later falling outside the Amendment’s protection because, “[a]lthough petitioner’s conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed”).
Intuitively, one would assume that information provided to secure Internet websites would be protected, especially in the case of electronic storage where the user is paying for a service that guarantees the security of information deposited. It may seem strange to think that this type of information disclosure could be considered exempt from Fourth Amendment protection, but it is at the very least plausible. On the other hand, there has been a strong case made for drawing a distinction between an automated recipient and an individual in applying the Third Party Doctrine. That argument contends the Fourth Amendment should protect information transmitted through the Internet to automated equipment run by third parties because the information is not being disclosed to a human being. For the purposes of this Comment, I will assume that the Court, if presented with the issue, would exempt all Level I social media use from the Third Party Doctrine. Such a conclusion seems intuitive and the alternative is undesirable because it would be to eliminate all privacy protection in Internet usage. Most of all, making the assumption leads to the more interesting question regarding the third stage of third party disclosure.

The third stage of third party disclosure in social media is more intriguing because it necessarily involves allowing a third party to view the information, while at the same time allowing the user to dictate who is a member of that third party. Although social media sites cannot be completely depended on to ensure the security of what it

103 See Petrashek, supra note 16, at 1520 (“The distinction between content and non-content information breaks down even further on the Internet, where ‘[u]sers disclose both content and routing information, in exactly the same technical manner, to an enormous number of third parties.’”).

104 See Timothy Lee, Why the ‘Third Party Doctrine’ Undermines Online Privacy Protection, TECHDIRT (June 20, 2008) available at http://www.techdirt.com/articles/20080530/201471272.shtml (“[W]e now entrust a host of private data—including our email, cell phone calling data, credit card transactions, and more—to private companies, and [that] the third party doctrine would seem to suggest that Fourth Amendment protections would not extend to such information.”).

105 See Matthew Tokson, Automation and the Fourth Amendment, 96 IOWA L. REV. 581, 585–86 (2011) (arguing that the ‘courts’ failure to distinguish between the disclosure of personal information to automated equipment and disclosure of to a human being” is potentially devastating to the Fourth Amendment’s privacy protection in the digital age).

106 See id. at 616 (arguing that many of the Supreme Court cases regarding the Fourth Amendment support the conclusion that the third party requires disclosure to a human being, and that the majority of information passed through the Internet is stored by third party automated servers and is never reviewed by a human being).

107 See id. at 602 (noting that because “virtually every kind of personal online data is stored and processed by third-party automated equipment,” if the Third Party Doctrine applies there will be no expectation of privacy in online communications).
posted,\textsuperscript{108} most users feel they have some control over who can view their information.\textsuperscript{109} This ability to limit the audience would likely not be viewed as a sufficient means of curtailing the applicability of the Third Party Doctrine. Courts often defend the Third Party Doctrine on the grounds that one who discloses information to a third party “assumes the risk” and, therefore, should not be entitled to constitutional protection.\textsuperscript{110} The same assumption of risk justification will likely be employed to defend applying the Third Party Doctrine to social media. Therefore, it is likely that the Third Party Doctrine would apply to all Level II and Level III type social media use.

Under current law regarding the Third Party Doctrine and the Internet, it appears Fourth Amendment privacy protection extends to the contents of electronic transmissions (e-mail, instant messaging, etc.), but not to their identification information (Internet Provider address, etc.). It also seems likely, but not definitive, that the Third Party Doctrine would not apply to information held in secure storage websites. Social media, however, has a third layer of third party disclosure, meaning it is even more unlikely that any content information provided to social media sites would be protected. It follows from this that, using my generalized categories, it is almost unquestionable that Level II and Level III social media use would be considered a waiver of Fourth Amendment privacy protection.

\textsuperscript{108} See Privacy Policy, FACEBOOK, http://www.facebook.com/note.php?note_id=%20322541825300 (last visited Nov. 23, 2011) (“Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.”).

\textsuperscript{109} A more complex issue that will not be discussed here is the transfer of information about the user to third party advertisers who tailor ads specific to a user’s interest. See Petrachek, supra note 16, at 1520 (“[I]nformation is not simply stored for the convenience of the web site user; instead the web site operators collect revenue by using this information to display ads tailored to the user’s particular interests.”).

\textsuperscript{110} See Kerr, supra note 93, at 564 (noting that the closest the Supreme Court has come to justifying the Third Party Doctrine is through the idea that someone who discloses to third parties assumes the risk that the information will not remain private).
B. Reasonableness of the Expectation

The Court’s decision in *City of Ontario v. Quon* has been criticized for failing to provide an update to the Fourth Amendment’s analytical framework for lower courts to apply to new technology in the employment context.\(^{111}\) Specifically, commentators attack the Court’s failure to address the discrepancy in *O’Connor* regarding the test for establishing the existence of a reasonable expectation,\(^ {112}\) instead choosing to decide the case on the grounds that even if there was a reasonable expectation of privacy, the search was ultimately reasonable and, therefore, not a violation of the Fourth Amendment.\(^ {113}\) For the purposes of social media, clarification is probably not needed because, under a straightforward application of either test, social media would likely not rise to the level of a reasonable expectation.

Both tests center on what can be called the “outside/inside distinction,”\(^ {114}\) a distinction dependent entirely on physical spatial factors for line-drawing purposes.\(^ {115}\) The “outside/inside distinction,” however, does not allow for either test to apply to social media use. First, the plurality’s approach in *O’Connor* centers on the nature of the workplace, specifically the spatial relationship the employee has with supervisors, in determining whether a reasonable expectation of privacy exists. Therefore, the employee’s expectation of privacy is assessed by “the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public—may have frequent access to an individual’s office.”\(^ {116}\) By focusing the analysis on the physical accessibility of the employee’s

---

\(^{111}\) See *Supreme Court, 2010 Term—Leading Cases*, 124 Harv. L. Rev. 179, 184–85 (2010) (arguing that the Court should have held that employees have no reasonable expectation of privacy in text messages, and a failure to do so “opened the door to *O’Connor*’s continued application in such circumstances and inevitably to inconsistent results on account of the flexibility of *O’Connor*’s fact-specific approach”).

\(^{112}\) See id. at 179 (“Yet instead of clarifying whether a government employee enjoys a reasonable expectation of privacy when using government-issued equipment, the Court provided no helpful guidance for similar cases in the future, declining to decide whether the Fourth Amendment provides such a reasonable expectation in technological contexts.”).

\(^{113}\) See *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010) (noting that it is not necessary to resolve the question of which *O’Connor* test is controlling because, “[t]he two *O’Connor* approaches—the plurality’s and Justice Scalia’s—therefore lead to the same result here”).

\(^{114}\) Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1010 (2010) (noting that the distinction between “surveillance outside and government surveillance inside is probably the foundational distinction in Fourth Amendment law,” and that any government intrusion in the “outside” area is not a Fourth Amendment violation).

\(^{115}\) See id. at 1011 (“In the physical world, the line that the Fourth Amendment protects is the line between inside and outside.”).

workplace, the Court fails to cover new technology because it does not factor in the accessibility of virtual information. Under this test, an employer will always be allowed access to an employer-owned computer and, therefore, the conduct of the employee on that computer will never amount to a reasonable expectation of privacy under the plurality’s approach.

Scalia’s approach offers no direct help to the problem of virtual privacy because his opinion also provides guidance for only tangible spatial standards. Scalia argues for clear and explicit areas, such as an office and drawers in an office, that necessarily have an expectation of privacy.\footnote{See \textit{id.} at 731 (Scalia, J., concurring) (“I would hold, therefore, that the offices of government employees, and \textit{a fortiori} the drawers and files within those offices, are covered by Fourth Amendment protections as a general matter.”).} Scalia, however, qualifies his proposal by asserting that this presumption of privacy can be defeated in situations where “the office is subject to unrestricted public access.”\footnote{\textit{Id.}} Under Scalia’s approach, privacy is still subject to the inside/outside distinction because the expectation of privacy is determined by the physical openness of the area in question. So long as the physical and spatial distinctions remain foremost in the analysis for employee privacy, there is likely no expectation of privacy in social media use.

\textbf{C. Balancing Test}

The Court in \textit{Quon} did not need to resolve the discrepancy regarding the threshold issue in applying the Fourth Amendment to public employees because it determined the search was justified. In doing so, the Court applied the second part of the Fourth Amendment analysis developed in \textit{O’Connor} used for evaluating when a government intrusion against public employees is sufficiently justified to trump the reasonable expectation of privacy.\footnote{City of Ontario v. Quon, 130 S. Ct. 2619, 2628–29 (2010).} In \textit{Quon}, the government employee had been issued a cell phone with a coverage plan that allowed for a specific number of text messages per month.\footnote{\textit{Id.} at 2625.} If the employee exceeded the limit of text messages, the employer would incur additional costs.\footnote{\textit{Id.}} The plaintiff, Quon, went over his allotted number of messages and, in an attempt to determine whether there was a need to upgrade the city’s service plan to allow for more text messages, the City performed an audit of his text messages to de-
termine how many were work related. In a review of those messages, the City discovered several sexually explicit messages sent by Quon during work hours and, as a result, Quon was disciplined. He brought suit claiming, among other things, that the review of the transcripts of the content of his text messages constituted an unreasonable search in violation of the Fourth Amendment. The Ninth Circuit agreed with Quon, holding both that Quon had a reasonable expectation of privacy in the text messages and that the search was “not reasonable in scope.” The Supreme Court overturned the Ninth Circuit, noting that it did not matter whether Quon had a reasonable expectation of privacy because the search was justified and reasonable in scope.

The Court held that the search was reasonable because the legitimate government interest outweighed the reasonableness of the expectation. The Court assessed the reasonableness of the search by balancing it against the privacy expectation of the individual. The Court found that the reasonableness of the expectation was not sufficient in large part because Quon was on notice as to the possibility of his employer reviewing his text messages. As evidence that Quon had a diminished expectation of privacy, the Court pointed to the City’s “Computer Usage, Internet and E-Mail Policy,” which stated, “[u]sers should have no expectation of privacy or confidentiality when using these resources.” Such policies are not novel and many employers now have Internet policies that give notice to the employee that the employer may monitor the employee’s Internet usage, including social media use. Therefore, based on the Court’s reliance on notice to the employee, coupled with the Court’s general deference given to public employers, it is unlikely that monitoring an employee’s social media use would be viewed as amounting to a sufficiently unjustifiable search, such that Fourth Amendment protection would apply.

122 Id. at 2626.
123 Id.
124 Id.
126 Quon, 130 S. Ct. at 2627–29.
127 See id. at 2632 (“Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the O’Connor plurality.”).
128 See id. at 2631 (“[T]he fact that Quon likely had only a limited privacy expectation . . . lessened the risk that the review would intrude on highly private details of Quon’s life.”).
129 Id. at 2625.
VI. THE CASE FOR SOCIAL MEDIA PROTECTION

“General suggestions that, in the current climate of ‘over-sharing’ on Facebook, MySpace, and Twitter, Americans have acquiesced to ‘the end of privacy,’ have been refuted by a number of recent events which reflect a growing trend towards maintaining and protecting privacy rights in an age of rapidly-evolving technology.”

Social media use by government employees should be protected under the Fourth Amendment because of changes in how the Internet is used. The Third Party Doctrine can no longer be employed as an effective limit on the expectation of privacy because social media has transformed society’s expectations of privacy. Secondly, the test for determining a reasonable expectation in the public employment context should divert from the physical/spatial line-drawing analysis. If this occurs, then the plurality’s approach in O’Connor should be formally adopted because it can adapt so as to include social media. Finally, determining if the expectation is sufficiently justified to warrant Fourth Amendment protection should be based on the security measures available and taken by the employee, and not based on whether there was sufficient notice provided by the employer.

A. Recognizing an Expectation of Privacy in Social Media: Rejecting the Application of the Third Party Doctrine

Changes in technology and society have created a need for a reevaluation of the Third Party Doctrine. Social media is founded on voluntary disclosure to third parties, so in the extreme one could consider all social media content as outside the scope of the Fourth Amendment. That does not, however, align with the reality of today’s world where people have as much of an expectation of privacy using these social media sites, much less the Internet, as they do using telephones or storage units. David Couillard expressed this sentiment by noting:

The Internet is constantly evolving. The increased speed and mobility of Internet access, and the more widespread usage of Internet services and digital information, makes the online cloud more than a public medium—it is an anywhere-access point for private data. Companies and individuals turn to the cloud as a convenient and cheap alternative to traditional hard drive storage, and society expects its photo albums, address books, calendars, documents, and emails to maintain the same protections on a secure account in the cloud as they would if stored on a home computer. The increased availability and usage of virtual con-

130 Plourde-Cole, supra note 35, at 624.
cealment tools, such as passwords, encryption, and unlisted links, makes these expectations of privacy subjectively reasonable.\textsuperscript{131}

Thus, it is imperative that the Court reassess, if not altogether abandon, the Third Party Doctrine in light of the advancements made in technology. Failure to do so could, arguably, lead to a situation where there no longer exists any "expectation" of privacy under the Fourth Amendment.\textsuperscript{132}

This is not to say that all Internet use should suddenly be granted an expectation of privacy. By assuming that the Third Party Doctrine does inherently remove all expectation of privacy in the Internet, however, we can begin to analyze the specific characteristics of different types of social media and determine whether a reasonable expectation should nonetheless exist based on the security features and who has access to the information. If a user limits the access to their online profile and/or information disseminated through a social media website, either by requiring a password or by allowing only certain other social media users to view the information, then they have an expectation that society is ready to recognize as reasonable. On the other hand, if an employee does not take advantage of the many security features available on most social media sites, their expectation is no longer reasonable. This acknowledgement, of the unique characteristics of differing types of social media use, does not necessarily require a complete overhaul or dissolution of the Third Party Doctrine. For example, a social media output, such as a Facebook post, whose viewers the user restricts, could be viewed as similar to a direct communication (such as a telephone conversation or e-mail). Under this interpretation, the Fourth Amendment would still be applicable unless one of the recipients (i.e., one of the user’s “friends”) volunteered the information to the public employer. Therefore, the Third Party Doctrine would not mean that an employee necessarily waives their Fourth Amendment protection just by posting information online, rather it would depend on the employer’s ability to access that information.

While this offers little guidance to employers and employees, or lower level courts for that matter, it does align with the Court’s opi-

\textsuperscript{131} Couillard, \textit{supra} note 2, at 2238.

\textsuperscript{132} \textit{See} Henderson, \textit{supra} note 99, at 562–63 ("The REP [(reasonable expectation of privacy)] test must be limited to reign in its third party doctrine. Without external restraint, technology will lead to an expectation of no privacy, and police practice will incorporate that technology to create a reality of no privacy. . . . Restricting the third party doctrine to information deliberately conveyed in order that its content be used is a necessary step in preventing the Fourth Amendment from becoming irrelevant.").
nion in *O'Connor* and *Katz*, whereby Fourth Amendment claims must be analyzed using a case-specific, fact-intensive inquiry. The point here is that the Court should not automatically dismiss social media use as outside the realm of Fourth Amendment protection based on its sharing component, but rather analyze on a case-by-case basis whether an expectation of privacy exists as required under current Fourth Amendment doctrine. If viewed in this way, the Third Party Doctrine would apply only to Level III type social media use, leaving the possibility open for Level I and Level II type use to receive Fourth Amendment protection.

**B. Defining the Expectation: When Social Media Use Creates a Reasonable Expectation of Privacy**

Reassessing the application of the Third Party Doctrine is only part of the battle. The Court’s two tests offered in *O'Connor* are both based on physical and spatial boundaries, which means social media would likely fall outside the scope of Fourth Amendment protection. The inside/outside distinction, however, is no longer applicable to Fourth Amendment analysis due to changes in technology, so the tests should be viewed in a way that accounts for this change. Ultimately, the plurality approach in *O'Connor* is best suited to be adapted in such a way that will potentially allow the Fourth Amendment to cover social media.

The Court should move away from assessing Fourth Amendment privacy based on physical and spatial boundaries because information is becoming exclusively stored in the virtual world. This change must be reflected in the analysis the courts take in assessing a reasonable expectation of privacy. The Court, however, need not adopt a completely separate approach in light of this social transformation. The plurality approach could be adapted so as to include social media use. Under the plurality’s approach in *O'Connor*, social media could be incorporated if the focus moved away from the physical nature of the workplace and instead looked at the type of work involved. The

---

133 See *O'Connor* v. Ortega, 480 U.S. 709, 718 (1987) (“Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.”).

134 Scalia’s approach could be adapted to incorporate this change. His reasoning could be used to create strict guidelines for the virtual world as to what is and is not covered under the Fourth Amendment. This approach, however, would provide inadequate protections because the types of social media uses and security measures that are applied vary so drastically that any attempt to categorically apply the Fourth Amendment would be fruitless and would undoubtedly leave some areas without proper protection.
scope of protection would not depend on whether the physical nature of the workplace lends itself to the employer having a need to rummage through an employees workspace because the employer will always have a legitimate need to search a company-owned computer. Rather, the scope of protection would depend on the nature of the workplace with respect to online activity and the relationship the work has to certain types of social media sources. Accordingly, if the nature of the work performed by the employee is such that social media use substantially impacts the workplace or the employer, or if social media is an integral part of the work being done, then the employee would not retain a reasonable expectation of privacy. If, on the other hand, the nature of the work had no relationship to social media use, then the contents of Level I and Level II type social media use should contain a reasonable expectation of privacy.

Ultimately, the Court in Quon did not clarify which O’Connor test should be applied in determining expectations of privacy in the workplace. Such a clarification would help future courts grapple with the emergence of social media use in the workplace. Furthermore, based on the difficulties associated with applying the Fourth Amendment to social media use, the plurality’s approach in O’Connor would provide the best framework within which to assess employee Fourth Amendment privacy claims. In using that approach, however, the courts should acknowledge the change in technology that makes spatial distinctions inadequate.

C. Limiting Unreasonable Searches: Notice as a Non-Factor

If a reasonable expectation of privacy regarding social media use can be established it must also be able to survive O’Connor’s balancing test in order to constitute a Fourth Amendment violation. Currently, that test places a heavy emphasis on whether or not notice is provided to the employee, essentially allowing any reasonable expectation to be destroyed if sufficient notice is given. Notice, however, should not be a determinative factor in deciding the extent to which the expectation is reasonable because an employer should not be allowed to bypass an employee’s constitutional rights by merely providing advanced notice.135 Furthermore, notice does not exempt employers from liability under many of the federal statutes, such as the Electron-

135 See WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 10.8(a), at 335 (4th ed. 2004) ("The Fourth Amendment would be meaningless if the ‘expectation of privacy’ which it is intended to protect would be dissipated by nothing more than advance announcement by the government . . . ").
ic Communications Privacy Act, and so too should it not exempt them from constitutional violations. Thus, notice should be "simply a factor relevant to the analysis and not the final indication of what privacy an employee can expect."

Unfortunately, in the aftermath of *O'Connor*, the lower courts have chosen to utilize notice as a bright line rule for valuing the reasonableness of an employee’s expectation against the interest of the employer. In *United States v. Simons*, the Fourth Circuit upheld a search of a computer of an employee for the Foreign Bureau of Information Services ("FBIS"). The Fourth Circuit based its reasoning on the existence of an employer Internet policy that provided the employee with notice that Internet use on employer-owned equipment was subject to search. Conversely, in *United States v. Slanina*, the Fifth Circuit found that the employee had a reasonable expectation of privacy in his employer-owned computer based on the lack of an employee policy. The Fifth Circuit held that there was a reasonable expectation of privacy "given the absence of a city policy placing [defendant] on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer." These cases illustrate the trend, continued in *Quon*, towards applying a clear, all or nothing approach to the balancing test laid out in *O'Connor*. This heavy emphasis on notice, to the point of becoming an absolute defense to employee Fourth Amendment

---

136 See Lazar et al., *supra* note 55, at 228 ("Employers’ technology policies do not give carte blanche access to employees’ personal electronic information . . . .").

137 Hess, *supra* note 26, at 276.

138 See id. at 276–77 ("The original balancing test created by the Supreme Court in [*O'Connor*] has eroded into a bright line rule that stresses convenience and ease of administration over constitutionally protected rights.").

139 United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) (concluding that "FBIS’s searches of Simons’ computer and office did not violate Simons’ Fourth Amendment rights").

140 See id. at 398 ("[I]n light of the Internet policy, [defendant] lacked a legitimate expectation of privacy in the files downloaded from the Internet."); see also Hess, *supra* note 26, at 274 ("The policy in place at the FBIS negated [defendant’s] subjective expectation of privacy in his computer and allowed his employer to circumvent the protections afforded [defendant] by the Fourth Amendment.").

141 United States v. Slanina, 283 F.3d 670 (5th Cir. 2002).

142 Id. at 677.

143 In all these cases the information that the employer obtained had been downloaded to employer-owned equipment. It is, therefore, unclear whether the Court would determine that an employer can negate an employee’s reasonable expectation by provide notice of searches of external websites accessed through employer-owned equipment. The trend in the case law, however, suggests that it would.
claims, is inconsistent with the case-by-case, fact-specific balancing approach intended by the O’Connor plurality.\textsuperscript{144}

Based on the way social media is used in today’s society and the way people perceive it as a conduit for transmitting and storing information, the courts should evaluate an individual’s reasonable expectation of privacy in regards to information provided to social media sites by looking at how that information is protected by the user. The weight of the expectation should vary depending on the security measures taken by the user and not the notice provided by the employer. Courts need to acknowledge the reality that Internet use is no longer inherently public and that there is a multitude of different measures individual’s can take to secure their online information. Thus, the more relevant factor should be the security measures taken by the employee, as opposed to the notice provided by the employer.

D. The New Approach: Putting It All Together

The new approach offered in this Comment does not seek to supplant the current Fourth Amendment doctrine as applied to public employees. Rather, it incorporates the realities of current Internet use and attempts to provide employees with only the amount of privacy protection that society has come to accept as reasonable. This approach is more squarely aligned with Katz than an approach that precludes social media use from protection for any of the reasons discussed in Part VI.

First, the Fourth Amendment will not cover Level III social media use because of the Third Party Doctrine. If an employee takes no steps to shield their social media content from the general public, he or she has waived any claim of privacy. Almost all Twitter, comment postings on third party websites and blog usage will not be covered because there is no expectation of privacy. On the other hand, Level I social media use will always have an expectation of privacy. Therefore, Facebook messages, other forms of direct communication and any electronic storage on an external site will be protected even if the employee uses an employer-owned computer.

Finally, under this approach Level II social media use will be the battleground of employment litigation. Level II social media use will

\textsuperscript{144} See Hess, \textit{supra} note 26, at 275 ("[Notice], however, was not the only factor Justice O’Connor listed for courts to consider when evaluating an employee’s privacy expectation . . . . By stressing that employees’ privacy expectations must be determined on a case-by-case basis, the plurality in \textit{O’Connor} sought to avoid a bright line test in evaluating privacy expectations.").
likely have an expectation of privacy, unless the type of employment is such that social media use is an integral part of employment. A government employee charged with maintaining a social media webpage, for example, most likely will not have an expectation of privacy as to their own profile on that same site due to the nature of their work. On the other hand, an accounting employee whose social media use has no impact on his or her employment can reasonably expect that his or her social media use is private. That expectation, however, can be defeated by showing the employee did not take appropriate steps to secure the information contained on the social media site. So if the accounting employee failed to properly secure his or her Facebook or MySpace profile, the legitimate interests of the government could be sufficient to trump his or her expectation of privacy.

VII. CRITIQUE

"Contrary to popular belief, new technologies are not the cause of eroding privacy in our society . . . ."145

The obvious question to ask even if one were to accept that employees’ social media use could be protected by the Fourth Amendment is whether, as a normative matter, it should be? This question is the foundation of several objections to expanding the Fourth Amendment to protect employee social media use. One such argument is that social media use does not need to be protected because technology advances have made it sufficiently difficult for employers to monitor this activity. As one scholar explains,

over the past one hundred and fifty years, new technologies have for the most part enhanced our privacy, and many of the invasive surveillance technologies that the government now uses are simply a response to this enhanced level of privacy—that is, an attempt to return to the former balance between individual privacy and [government] needs.146

Thus, the scope of the Fourth Amendment’s privacy protection should be curtailed, not expanded, in the wake of new technology.

To some degree this argument has merit in the context of social media. It is true that technology continues to provide new and more secure ways of protecting information on those sites. But that alone does not license the government, in its capacity as employer, to infringe on what has become a fundamental right. The employer’s

146 Id. at 531.
concerns are legitimate, but surely technology equally allows for employers to adequately protect themselves without the need for unrestricted access to online content posted by their employees.

Another reason to protest the expansion of privacy protections is the detrimental impact it may have on other substantial interests. This argument was made to the Court in *Quon*. The defendant called for limiting the application of the Fourth Amendment based on the government’s responsibility to the public. The claim was that because “government employees often have a powerful ability to affect the lives of the citizens with whom they interact . . . governmental agencies have an obligation to monitor their employees’ activities.”

Under this rationale, the duty government employers owe to the public to monitor employees’ social media outweighs their right to privacy.

This objection has greater merit in the wake of WikiLeaks, but it is just an extension of a historic argument against Fourth Amendment protection for government employees. The argument that the public good is best served by allowing government employers to conduct business in a way that is efficient and protects the public would defeat all Fourth Amendment protections for government employees. That is not the approach the Court has chosen. My argument states that if the Court is going to extend Fourth Amendment protections to government employees, then these protections should include those employees use of social media. While it may be rare that the content and the manner in which someone puts out information on a social media site outweighs the government’s interest in monitoring its employees, that does not mean the protection should never exist. The Fourth Amendment was designed to prevent government from being overly intrusive in our daily lives. To retain this purpose, it must extend to employee information on social media websites because that is how the modern employee stores and communicates information.

---


148 See id. (arguing that the obligations to the public “undercut any public employee’s claim to privacy in electric communications conducted on government-issued equipment”).
CONCLUSION

“The Internet has provided a dramatic change in societal conditions and the Fourth Amendment should not be lost in cyberspace. Society, speaking through its voice in Congress has shown that it objectively expects more protection from the Fourth Amendment than the Supreme Court, in the past, has been willing to give.”

There can no longer be any denying social media’s extreme prevalence and importance in our society. In deciding Quon without resolving which O’Connor test will be used to determine the reasonableness of an employee’s expectation of privacy, the Court left uncertain how the Fourth Amendment will apply to the variety of ways the Internet is now being used. Accordingly, we are left to speculate as to how this issue will one day be resolved. There are obvious problems with attempting to outline new approaches to new technology before seeing how the technology will ultimately be incorporated into society. As Justice Kennedy cautioned, “[t]he Court must proceed with care when considering the whole concept of privacy expectations . . . [t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.” The opinion of Quon, however, leaves both employers and employees with little guidance on how to structure their relationships in light of social media’s widespread use. Furthermore, based solely on past decisions, it appears as though the Fourth Amendment would not cover social media, and that does not square with the reality of today’s society.

150 Quon, 130 S. Ct. at 2629.