UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 10
Issue 1 *Fall 2008*

Article 6

10-1-2008

Tag - Now You're Really It What Photographs on Social Networking Sites Mean for the Fourth Amendment

Daniel Findlay

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 10, ISSUE 1: FALL 2008

TAG! NOW YOU'RE REALLY "IT"
WHAT PHOTOGRAPHS ON SOCIAL NETWORKING SITES MEAN FOR THE FOURTH AMENDMENT

Daniel Findlay [1]

Now that mobile technological devices like camera phones pervade our world, allowing people to capture images and scenes in places and at times never before possible, serious privacy concerns inevitably arise. The fact that users of social networking sites, which are growing rapidly in popularity, frequently and commonly propagate these easily captured images, as well as traditional ones, throughout cyberspace with startling ease only serves to bolster such threats to personal privacy. Transforming threat to reality, law enforcement officers search these online sites and use the photographs posted to them to help effect significant legal consequences. Given such staggering new social dynamics, novel legal questions emerge regarding what privacy expectations exist in the social conscience of today's technologically hip world as well as whether traditional privacy formulations and the guarantees of the Fourth Amendment are adequately equipped to protect those expectations. In light of the various and harsh penalties that can arise from users' ability to post and widely share photographs of others both with and without those people's knowledge, the government's accessing and use of such photographs could, under certain circumstances, constitute constitutionally unwarranted invasions of privacy.

I. INTRODUCTION

Henry had a great night ahead of him—he and his college roommates were throwing a small party with their close friends to celebrate the start of the college football season. The night did not

[1] J.D. Candidate, University of North Carolina School of Law, 2010.

disappoint; Henry grilled some delicious steaks, the home team won handedly, and the guests enjoyed each other's company and a surplus of beer and wine deep into the night. Everything was perfect. Or so Henry thought.

A few days following the party, police knocked on Henry's door and informed Henry that the state was criminally prosecuting him for providing alcohol to minors.[2] It turns out that one of the party guests had posted a photograph album from the party on a social networking website.[3] A fellow student with an axe to grind saw the photographs of Henry providing drinks to underage classmates (unbeknownst to Henry) and thereafter tipped off the police. Unaware that the photographs had even been taken, much less posted online, Henry felt hurt and betrayed because he was identified as the lone culprit when other people had performed the same act. Was the use of such photographs impermissible by law in any way? Had Henry's privacy been improperly invaded?[4] By whom?[5]

---

[2] Similar actions have been taken or threatened in the education context by numerous schools across the country. Student users of social networking sites have been expelled for online criticisms of school officials, written up for alcohol consumption in on-campus dorms, disciplined for other illegal activities like under-age drinking, investigated for political statements, as well as identified and punished for unruly and disorderly behavior. *See* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement, Dec. 14, 2005, at 4A, *available at* http://www.nytimes.com/2006/01/08/education/edlife/ facebooks.html (last visited Nov. 14, 2008). *See also* Harvey Jones & José Hiram Soltren, *Facebook: Threats to Privacy*, MASS. INST. TECH. at 30 (2005) (discussing the expulsion of Cameron Walker at Fisher College due to an online group he created to criticize a campus security officer), *available at* http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (last visited Nov. 14, 2008); Matthew J. Hodge, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L. J. 95, 95 (2006).

[3] *See* John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1220 (2007) (stating that social networking sites, in their most basic formulation, are online communities consisting of networks of individuals connected and linked through personalized web "profiles").

[4] The notion of a "right to privacy," insofar as such an entitlement operates to secure the "protection of the person" or the "right to be let alone," was first postulated in the regime of tort law by preeminent legal scholars Samuel Warren

The surging role of social networking sites like Facebook[6] and MySpace,[7] especially among teenagers,[8] tests the boundaries of

---

and Lewis Brandeis in an 1890 article and has evolved from this famed beginning. Samuel D. Warren & Lewis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 195 (1890). Notably though, it was "[r]ecent inventions and business methods," including "instantaneous photographs" and "numerous mechanical devices" which first "call[ed] attention to the next step" in securing or at least better ensuring personal protection. *Id.* The circumstances which prompt a discussion of the right to privacy as it exists (or perhaps should exist) amid today's novel technological landscape appear to mirror those triggering circumstances that led to the discussion of such a right's existence originally. *See also* Patricia Sanchez Abril, *Recasting Privacy Torts In A Spaceless World,* 21 HARV. J. L. & TECH. 1, 11 (2007).

[5] With respect to direct liability, the social networking site itself is absolved from any exposure under the Communications Decency Act, provided that: (1) the information in question originated independently from a user; and (2) the site executed no editorial or heightened review function; *see* 47 U.S.C. § 30(c)(1) (1996). *See also* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 293 (D.N.H. 2008), *reconsideration denied by* Doe v. Friendfinder Network, Inc., 2008 U.S. Dist. LEXIS 38177 (D.N.H. 2008) ("Under the Communications Decency Act ("CDA") . . . '[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider' . . .").

[6] Facebook, http://www.facebook.com (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology). The most popular social networking site worldwide, grouping users into online communities where they can associate with "friends," publish customized personal information, and communicate with other users. *See* Wilson, *supra* note 3, at 1204; Hodge, *supra* note 2, at 98–99.

[7] MySpace, http://www.myspace.com (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology). The second most popular social networking site, performing the same basic functions as Facebook. *See* Kenneth Corbin, *Facebook Tops MySpace as Social Sites Globalize*, INTERNETNEWS.COM, Aug. 14, 2008, http://www.internetnews.com/webcontent/article.php/3765406/Facebook+Tops+MySpace+as+Social+Sites+Globalize.htm(citing comScore metrics analysis) (last visited Nov. 14, 2008) (on file the with the North Carolina Journal of Law & Technology); Hodge, *supra* note 2, at 98–99.

[8] *See* Abril, *supra* note 4, at 13 (citing recent poll by the Pew Internet Project, which found that 55 percent of Internet users from ages twelve to seventeen have profiles on online networking websites); Amanda Lenhart & Mary Madden, *Teens, Privacy & Online Social Networks*, PEW INTERNET & AMERICAN LIFE PROJECT, at ii (2007), *available at* http://www.pewinternet

traditional privacy recognitions on multiple fronts.[9] New concerns regarding which privacy expectations deserve protection emerge as it becomes easier for social network users to upload photographs of others without their knowledge, and sometimes without triggering any mechanism to put them on notice. Combined with the startling ease with which such photographs are accessed by the public (including law enforcement officers and public school officials), questions abound as to where those protections may be found in the law. Specifically, the pervasive practice of posting photographs on online networking sites raises questions regarding circumstances where state actors access and use such photographs without warrants and whether those circumstances violate a person's right to privacy.[10]

.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (last visited Nov. 16, 2008) (on file with the North Carolina Journal of Law & Technology).

[9] *See* Catherine Rampell, *What Facebook Knows That You Don't*, WASH. POST, Feb. 23, 2008, at A15, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/22/AR2008022202630.html (last visited Nov. 16, 2008); Chris Soghoian, *Exclusive: The Next Facebook Privacy Scandal*, CNET News, Jan. 23, 2008, http://news.cnet.com/8301-13739_3-9854409-46.html (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology); Jeffery R. Young, *Study Raises New Privacy Concerns About Facebook*, THE CHRON. OF HIGHER EDUC., Feb. 4, 2008, *available at* http://chronicle.com/free/2008/02/1489n.htm (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology); Associated Press, *Facebook Feature Draws Privacy Concerns*, MSNBC.COM, Sept. 8, 2006, http://www.msnbc.msn.com/id/14728756/ (on file with the North Carolina Journal of Law & Technology). *See generally* Harvey Jones & José Hiram Soltren, *Facebook: Threats to Privacy*, MASS. INST. TECH. at 1–41 (2005), *available at* http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (last visited Nov. 14, 2008); *Criticism of Facebook: Privacy Concerns*, Wikipedia—The Free Encyclopedia, http://en.wikipedia .org/wiki/Criticism_of_ Facebook#Privacy_concerns (last visited Nov. 17, 2008) (on file with the North Carolina Journal of Law & Technology).

[10] In a string of cases spanning most of the 20th century, the United States Supreme Court gradually illuminated areas of "privacy rights" or "liberty interests" that it controversially found embedded in the Constitution—with justifications ranging from "penumbras" and "emanations" of the Bill of Rights to a vague "zone of privacy" as well as Ninth and Fourteenth Amendment rationalizations. *See generally Exploring Constitutional Conflicts: The Right of Privacy*, University of Missouri-Kansas City School of Law, http://www.law

Contemporary standards for defining privacy should be crafted to reflect an increasingly integrated and interactive world where people often voluntarily engage in situations with fewer barriers protecting their privacy. In other words, what the reasonable person today considers private requires new or evolved paradigms. Moreover, advancements in technology—such as pocket-sized digital cameras, camera phones,[11] and social networking sites[12]—propel both the taking and dissemination of photographs to new realms. This makes traditional protection mechanisms and means of controlling privacy outdated in many respects. These real-world developments require a nuanced inspection of the Fourth Amendment's application to such a context. In light of the ways people currently use social networking websites and the expectations they reasonably attach to their actions therein, certain actions by government officers in accessing photographs could constitute unconstitutional searches and seizures violating the right to privacy secured by the Fourth Amendment.

This Recent Development explores and highlights how the scope and usage patterns of photographs posted on social networking sites challenge the existing notions of privacy expectations within the confines of the Fourth Amendment and government searches and seizures. First, Part II highlights the recent and expansive use of photographs gathered from social networking sites in legal contexts and details how these trends

---

.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (last visited Oct. 15, 2008) (on file with the North Carolina Journal of Law & Technology).

[11] *See* Jeremy Cothran, *Athletes' 'Images' Always at Risk: Nowhere to Hide in this High-Tech Age*, THE STAR-LEDGER, Sept. 13, 2008, at Sports 1, http://www.nj.com/mets/index.ssf/2008/09/athletes_images_always_at_risk.html (quoting Derek Jeter regarding the pervasiveness and tricky issues posed by camera phones: "Now everyone's got it in a phone, so everywhere you go, everything you do, you've just got to have the philosophy or the mind-set that they're watching") (last visited Oct. 13, 2008) (on file with the North Carolina Journal of Law & Technology).

[12] Facebook, http://www.facebook.com (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology); MySpace, http://www.myspace.com (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

present unprecedented issues that may not comfortably fit in existing Fourth Amendment paradigms. Next, Part III outlines how photographs are used on social networking sites and explains what user-enabled privacy protections currently exist as well as ones that do not. Part IV provides a brief overview of the Fourth Amendment and the privacy entitlements possibly secured therein. Then, Part V examines traditional Fourth Amendment privacy law conceptions as they apply to the current social networking site dynamics and discusses how the new environment created by these online communities forces new considerations as to what types of searches are constitutionally warranted. Finally, Part VI offers a reasoned forecast about the future of privacy law generally in a digital social networking world.

II. RECENT FORAYS FOR PHOTOGRAPHS POSTED TO SOCIAL NETWORKING SITES

While the straightforward use of online photographs[13] to implicate a guilty party is itself a recent innovation in the legal world,[14] it has already spurred other developments. Numerous new applications of photographs are arising throughout the various arenas of law, all of which raise questions about potential violations of rational privacy expectations or possible extensions of such expectations.[15] Further enriching the complexity of the issue

---

[13] Social networking sites also allow the posting of videos, a medium which presents largely identical legal issues as does the posting of photographs (while also possibly adding interesting and important contextual information). *See Facebook: Videos*, http://www.facebook.com/help.php?ref=pf (last visited Nov. 17, 2008) (on file with the North Carolina Journal of Law & Technology).

[14] *See* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement, at 4A (pointing out how photographs have been used to directly legally implicate their subjects in various settings) *available at* http://www.nytimes.com/2006/01/08/education/edlife/facebooks.html (last visited Nov. 14, 2008).

[15] In addition to this Recent Development's specific Fourth Amendment search-and-seizure concerns, the evolving social dynamic may present possible tort claims, along with attaching liability, for users posting and tagging online photographs; as well as possible *Bivens* and/or 42 U.S.C. § 1983 claims against government actors. *See* Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. LAW & TECH. 1 (2007).

is the fact that the subject matter here involves photographs,[16] which are undeniably accurate depictions of a singular moment in time (assuming no digital alteration occurred). The coalescence of these issues ignites a fascinating inquiry as to whether a law officer's access, without a warrant, of photographs posted to a social networking site ever unlawfully intrudes on a recognizable user right to privacy.

Photographs taken from Facebook played an important role in a recent Rhode Island criminal case. There, the prosecutor handling a drunken-driving case presented pictures of the defendant at a party just two weeks after the accident.[17] Though the defendant himself was not responsible for posting the photographs,[18] the prosecutor introduced a picture of the defendant dressed like a prisoner with a shirt that read "Jail Bird" to paint the defendant as an "unrepentant partier who lived it up while his victim recovered in the hospital."[19] The judge in the case agreed, swayed in part by the pictures, which he characterized as depraved.[20] He sentenced the defendant to two years in prison.[21] The judge stated, "I did feel that gave me some indication of how that young man was feeling a short time after a near-fatal accident, that he thought it was appropriate to joke and mock about the possibility of going to prison."[22]

---

[16] Although the instant analysis specifically focuses on the use of photographs, the creation of party "invitations" on social networking sites has been introduced in a criminal case as evidence that the party organizers knowingly provided underage guests with alcohol. *See* State v. Tonelli, 749 N.W.2d 689, 690 (Iowa 2008), *reh'g denied* by State v. Tonelli, 2008 Iowa Sup. LEXIS 88 (Iowa June 10, 2008).

[17] Associated Press, *Unrepentant on Facebook? Expect Jail Time*, CNN.COM, July 18, 2008, http://www.cnn.com/2008/CRIME/07/18/facebook.evidence.ap/index.html (on file with the North Carolina Journal of Law & Technology).

[18] *Id.* Another victim in the crash saw the photographs on the defendant's Facebook page and provided them to prosecutors. *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

Drunk-driving defendants in California suffered similar sentencing fates due to photographs that depicted them in an embarrassing light, making it difficult for them to convince the judges that they were sufficiently remorseful or suggest that their illegal actions were not aberrations.[23] Photographs posted to online social communities are being applied in a variety of other legal contexts as well.[24] Those contexts involving police

---

[23] *Id.*

[24] One of the more interesting examples of this phenomenon took place recently in North Carolina where a personal injury plaintiff seeking ten million dollars in damages in a negligence suit received a judgment for absolutely nothing following a cross-examination in which photographs from her own MySpace page were used to poke holes in her case. Oldham v. Jackson and Smith Excavating, Inc. No. 06-CVS-642 (Chatham County Super. Ct., June 11, 2008); *see also* Guy Loranger, *MySpace Photographs Used Against North Carolina Injury Plaintiff*, N.C. LAW. WKLY., June 30, 2008, at 1. The jury delivered the verdict after just thirty minutes of deliberation. Photographs of the party-going plaintiff presented forceful evidence against her claims that the brain injury she suffered had so severely impacted her life and curtailed her activities that she could never achieve her dream of becoming a teacher. *See* Loranger, *supra*. As the defense attorney in that case said, the photographs "took away the sympathy effect." *Id.* In large part because of the clarity, forcefulness and irrefutability inherently provided by such photographs, litigators are increasingly using data-mining from social networking sites in depositions and for witness and litigant testimony.

A Delaware family court case illuminates possible extensions to the theme. In that case, photographs posted to an online social networking site showing a teenage boy and friends drinking at the boy's mother's house were introduced by the boy's father as evidence of improper supervision by the mother in an attempt to establish her lack of fitness as a parent. *See* N.P. v. J.P., 2008 Del. Fam. Ct. LEXIS 45 (Del. Fam. Ct. Jan. 30, 2008). Social networking websites and information posted on the Internet have also been used as a key part of the process for vetting jurors. *See* Julie Kay, *Social Networking Sites Help Vet Jurors*, THE NAT'L L.J., Aug. 13, 2008, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202423725315&rss=ltn (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology) (referencing U.S. v. Hassoun, No. 0:04-cr-60001 (S.D. Fla. 2006), *available at*, http://www.pegc.us/archive/US_v_Padilla/def_reply1_20061201.pdf) (last visited Nov. 14, 2008)) as an instance where a juror was dismissed after an online discovery showed she had lied on her jury questionnaire. Jury consultants are increasingly using these methods because "such sites are a treasure trove of information about potential and seated jurors that can be used

investigations of potential law breakers[25] and school officials monitoring the activities of their students[26] and their student athletes[27] most directly implicate the Fourth Amendment. Inevitably, such scenarios resound with privacy implications. It is a practical reality in the digital age, as one Illinois police officer stated, that "[i]f you don't want it to be my business, then don't post it?"[28] Or, alternatively, might the reach of the Fourth Amendment operate to bar certain government uses of online photographs, at least when those photographs are not posted by their subjects?

---

in picking the right jurors, bouncing potential jurors and even influencing jurors through the trial and in closing arguments." Kay, *supra*.

[25] *See* Stephanie Perry, *Can Facebook Lead to Your Arrest?*, THE DAILY FREE PRESS—BOSTON UNIV., Jan. 25, 2006, cached version from Sept. 20, 2008, *available at*, Google search for "Can Facebook Lead to Your Arrest," or *available at*, http://74.125.45.104/search?q=cache:PbKJ2CGQ5EwJ:www.dailyfreepress.com/media/paper87/news/2006/01/25/News/Can-Facebook.Lead.To.Your.Arrest-1504305.shtml+Can+Facebook+lead+to+your+arrest&hl=en&ct=clnk&cd=2&gl=us&client=firefox-a (discussing various incidents of police utilizing online photographs to aid their investigations) (last visited Oct. 14, 2008) (on file with the North Carolina Journal of Law & Technology). *See generally* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement at 4A (recounting, among other observations, a humorous anecdote where students suspected campus police were monitoring them online and staged a fake party, which the police came to break up), *available at* http://www.nytimes.com/2006/01/08/education/edlife/facebooks.html (last visited Nov. 14, 2008).

[26] *See* Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, Tech Support at 6 (mentioning a high school principal who saw online photos of partying students, and doled out punishment to those who were holding beer bottles but not to those with red plastic cups), *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html (last visited Nov. 14, 2008).

[27] Jimmy Greenfield & David Haugh, *When What Happens on MySpace Doesn't Stay on MySpace*, CHI. TRIB., Mar. 28, 2006, at 7 (noting a 10-day, delete-your-facebook-account-or-else policy issued to athletes at Florida State University and a mass email warning sent to athletes at Baylor).

[28] *Id.*

III. SOCIAL NETWORKING SITES

Social networking sites link networks of individuals into online communities through personalized web "profiles."[29] Users customize and publish their profiles, which often include the ability to "post" or "upload" written content, photographs, videos, music, and more.[30] Frequently, users communicate with each other via various messaging systems (with such communications occurring either privately or publicly), establish online "friend" networks,[31] and join groups based on common interests.[32]

Though these social networks are relatively new,[33] their growth has been astronomical. In June 2008, Facebook became the most widely used social networking site in the world, with approximately 132 million visitors worldwide.[34] Considering that this figure represents a 153 percent increase from the previous year,[35] the potential for continued growth appears robust to say the least.[36] MySpace, the industry leader as of 2007[37] (and still the

---

[29] John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1220 (2007).

[30] *Id.*

[31] *See id.* at 1220 n.90 (using quotations around "friend" denotes the fact that many users have little to no contact with some of their online "friends").

[32] *Id.* at 1220.

[33] Mark Zuckerburg launched Facebook in February 2004, while MySpace founders Tom Anderson and Chris DeWolfe created their site in July 2003. *Id.* at 1221–22.

[34] Kenneth Corbin, *Facebook Tops MySpace as Social Sites Globalize*, INTERNETNEWS.COM, Aug. 14, 2008, http://www.internetnews.com/webcontent/article.php/3765406/Facebook+Tops+MySpace+as+Social+Sites+Globalize.htm) (citing comScore metrics analysis) (last visited Oct. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

[35] *Id.*

[36] Triston McIntyre, *Facebook Usage Down, MySpace Still Top Dog*, BLORGE, May 20, 2008, http://tech.blorge.com/Structure:%20/2008/05/20/facebook-usage-down-myspace-still-top-dog/ (reasoning that Facebook's image as "hipper" and "younger" as well as its substantial base of college-aged users explains why it is considered a "more valuable entity") (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

[37] Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007), *affirmed by* Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008), *writ of cert. denied* by Doe v. MySpace, Inc., 2008 U.S. LEXIS 8516 (U.S. Nov. 17, 2008).

narrow leader in the United States[38]), counted more than 117 million global users as of June 2008.[39] In fact, social networking sites grew by twenty-five percent collectively over the past year,[40] and both MySpace and Facebook currently rank in the top five most popular sites overall in the United States, putting them squarely among Internet heavyweights Yahoo! and Google.[41] This enormous number of users, combined with their heavy usage,[42] shows the pervasiveness of such sites as part of modern-day life.

A. *Posting Photographs Online*

The photograph-posting process is a relatively simple endeavor. On Facebook,[43] for example, users simply login to the site, perform a one-time installation of a small enabling application, enter the folder directory on their computer where the photographs they want to upload are stored, and click upload.[44] At that point, the photographs are technically "online," though they may not be "live" in the sense that anyone is able to view them since the links that make the photographs readily accessible are not automatically formed. That is because Facebook allows users to

---

[38] *Top Sites: United States,* ALEXA, http://www.alexa.com/site/ds/top_sites?cc=US&ts_mode=country&lang=none (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

[39] Corbin, *supra* note 34.

[40] *Id.*

[41] *Top Sites*, *supra* note 38.

[42] According to Chris Hughes, a spokesman for Facebook, nearly three-quarters of the site's users sign on at least once every twenty-four hours, and the average user signs on six times a day. *See* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement at 4A, *available at* http://www .nytimes.com/2006/01/08/education/edlife/facebooks.html.

[43] "According to comScore, Facebook has the No. 1 photo service on the Web—thanks in part to its tagging feature . . . ." Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, Tech Support at 6, *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html.

[44] *See Facebook: Help Center,* http://www.facebook.com/help/seeall.php?facebook&id=412 (click on "How do I add photos and create an album?") (last visited Nov. 18, 2008) (on file with the North Carolina Journal of Law & Technology).

restrict (or at least attempt to restrict) the audiences that are permitted access to their photographs via individual, user-controlled privacy settings.[45] But many users do not avail themselves of these privacy controls.[46] Further complicating the issue, even Facebook asserts that "no security measures are perfect or impenetrable . . . [and that Facebook] cannot and do[es] not guarantee that User Content you post on the Site will not be viewed by unauthorized persons."[47]

B. *Tagging Photographs Online*

As another component of the photograph-posting process, users "tag," or place an identifying electronic marker, over people captured in the photographs. This labeling function allows viewers of the photographs to discover the identities of the people in the picture.[48] Additionally, Facebook provides the following four possible privacy settings that users can choose for each photograph album:

---

[45] *See Facebook: Help Center*, http://www.facebook.com/help.php (click on "Privacy") (last visited Oct. 7, 2008) (on file with the North Carolina Journal of Law & Technology); *see also* Hodge, *supra* note 2, at 98–99 (detailing the different privacy options for MySpace and Facebook).

[46] *See* Amanda Lenhart & Mary Madden, *Teens, Privacy & Online Social Networks*, PEW INTERNET & AMERICAN LIFE PROJECT, ii (2007) (reporting that more than a third of teen Internet users do not limit their profiles), *available at* http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf (last visited Nov. 16, 2008) (on file with the North Carolina Journal of Law & Technology).

[47] *Facebook: Privacy Policy*, http://www.facebook.com/policy.php (last visited Nov. 16, 2008) (on file with the North Carolina Journal of Law & Technology).

[48] In recent months, Facebook changed its photograph-tagging system to allow certain viewers of online albums to tag the subjects of the photographs they access—a practice referred to as "community tagging." This marked a shift from the previous system, in which the original uploader made the ultimate decision about who was tagged. Under the previous system, users were able to suggest people that should be tagged, but the original uploader had to confirm before links would be formed. Again, while not the precise focus of this Recent Development, such a change, in addition to implicating privacy expectations, may drastically expand who could potentially be liable for any harms resulting from *tagging*, since the number of people who can perform such an action on a given photograph has greatly increased.

> 1. Everyone: your friends and people on your networks can see photos in this album. Additionally, if you tag anyone in this album, the friends of the people you tag will be able to see the photos in which their friends are tagged regardless of which network they are on.
>
> 2. All my networks and all my friends: only the people on your networks and your friends will be allowed to see the photos in this album.
>
> 3. Some of my networks and all my friends: you can select which of your networks have permission to see the photos in this album. All of your friends will have permission to see the photos, regardless of their networks.
>
> 4. Only my friends: only your friends can see this album. These options are specific to each album, so different levels of privacy can be selected for different types of photos.[49]

These privacy settings—as well as the tagging process—are substantial measures which help curb violations of privacy. For example, the tagging process includes the vital component of notice. When a Facebook user is tagged, the tagged individual is notified of the action via email or other chosen means and can view the photograph and de-tag himself or herself. While this type of notice is offered, the fact that the link to the photograph forms immediately (and may be actively disseminated or "pushed" to other users by an automated Facebook "news-feed" process) means that the tagged individual is not granted any grace period for

---

[49] *Facebook: Help Center*, http://www.facebook.com/help/seeall.php?facebook&id=412 (click on "Who can see my photos?") (last visited Oct. 13, 2008) (on file with the North Carolina Journal of Law & Technology). Beyond these general settings, the uploader has the ability to share any given photograph (or album) with non-facebook users via a universal hyperlink. *See Facebook: Help Center*, http://www.facebook.com/help/seeall.php?facebook&id=412 (click on "How do I share my albums with people who do not use Facebook?") (last visited Nov. 14, 2008) (stating bluntly and opening the door to broad privacy concerns: "this link will always work, even if you add photos or change your album privacy settings") (on file with the North Carolina Journal of Law & Technology). Alternatively, users may limit the photos *they* post to their profile to their exclusive viewing or may completely deny access to specific, known individuals. *See Facebook: Help Center*, http://www.facebook.com/help/seeall.php?facebook&id=419 (click on "How do I restrict specific content from specific people?") (last visited Nov. 18, 2008) (on file with the North Carolina Journal of Law & Technology).

review. Thus, the subject is fully exposed to unrestrained potential invasions of privacy—including the prying eyes of law enforcement—until he or she receives the notifying email. While the action of de-tagging makes the photograph less discoverable with respect to the formerly tagged individual (because the photograph no longer appears linked in his or her profile), the photograph still remains online, and the person, while no longer identifiable by electronic marking information, continues to be at risk of independent visual verification by individual users.[50] What this means in reality is that one user may choose to de-tag himself or herself from a given picture because of privacy concerns, but if other people in the photograph remain tagged, the de-tagged individual is still subject to a high likelihood of unwanted publicity,[51] including possible exposure to probing government agents. Thus, while de-tagging offers some remedial protection, the protection is incomplete. A de-tagged individual remains in a predicament similar to that of a person captured in a photograph but never tagged—the lone advantage being that the once-tagged individual at least has knowledge of the photograph's existence and publication, whereas the never-tagged individual likely does not.

---

[50] Individuals can also be identified by plain text input by the original uploader, which does not create a link or trigger the automated sharing process, but also prevents the de-tagging process.

[51] Put differently, while an "incriminating" (used loosely) or "embarrassing" photograph may be removed from the implicated party's profile, the same people likely to discover and view it in the first place still have a good chance of discovering the photograph, whether through the profiles of the other tagged members or through other various means. Moreover, these viewers are often acquaintances of the de-tagged individual or at least familiar with him or her, and thus, the de-tagging action fails in its objective to prevent identification.

Though it receives as many as ten thousand complaints a day,[52] Facebook offers little help to users who may find themselves in such a scenario, claiming in its privacy policy that the best option for such circumstances is to ask the person who posted the photograph to remove it.[53] Asserting that "Facebook CANNOT make people remove photos that do not violate [Facebook's] Terms of Use,"[54] Facebook instead instructs dissatisfied users to avail themselves of the mercy of the original posters, who "should be respectful enough to remove unwanted photos."[55] In an ideal world, such rhetoric would put an end to the issue, but in the event the original poster proves uncooperative, problematic search and seizure issues arise.

IV. THE FOURTH AMENDMENT

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[56]

Historically, the amendment was read literally, so that any constitutional violation required "an official search and seizure of his person, or such a seizure of his . . . tangible material effects, or

---

[52] Karen Matthews, *Facebook, New York Attorney General Reach Agreement on Obscenity Safeguards*, ASSOCIATED PRESS, Oct. 16, 2007 (cached version from Oct. 17, 2007 available via Google search for "Facebook, New York attorney general reach agreement on obscenity safeguards" or at http://74.125.45.104/search?q=cache:tISiWTo6CPoJ:news.public.findlaw.com/ap/o/51/10-16-2007/f93e000982ccce7e.html+Facebook,+New+York+attorney+general+reach+agreement+on+obscenity+safeguards&hl=en&ct=clnk&cd=1&gl=us (last visited Nov. 17, 2008) (on file with the North Carolina Journal of Law & Technology).

[53] *Facebook: Help* Center, http://www.facebook.com/help/seeall.php?facebook&id=412 (click on "There's a photo of me on Facebook that I want taken down.") (last visited Oct. 13, 2008) (on file with the North Carolina Journal of Law & Technology).

[54] *Id.*

[55] *Id.*

[56] U.S. CONST. amend IV.

an actual physical invasion . . . for the purpose of making a seizure."[57] However, in 1967, partially owing to new factual paradigms brought about by changing societal circumstances,[58] the United States Supreme Court issued a landmark decision in *Katz v. United States*.[59] Critically, the Court recast the Fourth Amendment in recognition that "the Fourth Amendment protects people, not places."[60] *Katz*, along with its progeny, came to establish a two-step reasonableness standard as the analytical tool for evaluating Fourth Amendment privacy protections in the context of searches and seizures.[61] Thus, for constitutional safeguards to exist, "a person [must first] have exhibited an actual (subjective) expectation of privacy"[62] and, second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[63]

If both those elements are satisfied, "the police must acquire a warrant, with its corresponding probable cause requirement, to search the protected area or information in order comply with the Fourth Amendment."[64] Improperly collected evidence may be subject to the "exclusionary rule" and prove inadmissible.[65] These expectations have generally proven difficult to analyze in the age of the Internet. Courts have struggled to analogize the scenarios presented by cyberspace to considerations typically involved in determining traditional privacy expectations.[66] Even before the explosion of social networking sites and the accompanying photograph-posting phenomenon, courts had recognized that "[t]he advent of the electronic age and . . . the development of desktop

---

[57] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[58] *See id.* at 472–75 (Brandeis, J., dissenting).

[59] 389 U.S. 347 (1967) (including Justice Harlan's concurrence, *supra* note 61, which in many ways has come to shape and drive the current law of privacy).

[60] *Id.* at 351.

[61] Hodge, *supra* note 2, at 100.

[62] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[63] *Id.*

[64] *See generally* Hodge, *supra* note 2 (noting as well that exceptions to this requirement exist in certain circumstances).

[65] Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible").

[66] *See* Hodge, *supra* note 2, at 101–06.

computers . . . go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law."[67]

As a result, there is some inconsistency with regard to how courts have defined both subjective and objective privacy expectations in the digital age.[68] On one hand, the understanding exists that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[69] Accordingly, a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[70] Standing in contrast is the idea that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[71] Thus, it is unsurprising that privacy rights remain unsettled, especially as they relate to information contained on social networking websites, such as photographs posted by people other than their subjects. Email presents perhaps the most relative comparison to such information (though the parallel is somewhat forced and certainly not direct), and courts have reached conflicting decisions in determining whether reasonable privacy expectations attach to certain email communications.[72] Nevertheless, society seems interested in securing some privacy protections in the digital age; federal legislation and state court rulings have sought to expand privacy expectations.[73] In turn, this leads to the suggestion that, in light of society's contemporary working dynamics, general conceptions of what is considered "private" may also require expansion, significant alteration, or at the very least, clarification.

---

[67] United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).
[68] *See* Hodge, *supra* note 2, at 102–06.
[69] Smith v. Md., 442 U.S. 735, 743 (1979).
[70] United States v. Miller, 425 U.S. 435, 443 (1976).
[71] Katz v. United States, 389 U.S. 347, 351 (1967).
[72] *See* Hodge, *supra* note 2, at 104–06.
[73] *Id.* at 103–04.

V. EXISTING FOURTH AMENDMENT PRIVACY FORMULATIONS

The foremost concern of this Recent Development centers on the ability of social networking website users to post and widely share photographs of other users with and without their knowledge and whether the law enforcement agents or school officials who access or use these photographs without a warrant violate the Fourth Amendment's prohibition against illegal searches and seizures. The pristine ability of photographs to capture private moments in people's lives and then immediately communicate them to any and all viewers of their contents distinctly heightens the privacy issues involved. Thus, determining precisely how the unique environment created by the digital age fares under *Katz*'s two-prong privacy expectation test becomes critical.

A. *Subjective Expectation of Privacy*

In the context of photographs posted to social networking communities, this subjunctive *Katz* inquiry requires determination of whether the subject of any given posted photograph has a subjective expectation of privacy in that particular photograph. Making such a determination necessarily incorporates a myriad of factors. Key considerations would include: whether the photograph's subject even has knowledge of the photograph's existence, where the photograph was taken, who took the photograph, who posted the photograph, what device was used, what activities are documented in the photograph, why was the photograph taken, and the online privacy settings of both the uploader and the subject. Though these factors would unavoidably vary from photograph to photograph and person to person, it is not hard to conceive a variety of situations in which the necessary subjective expectation could exist for a given social network user. In other words, many hypothetical as well as real instances exist in which a given photograph subject could sufficiently seek to preserve the photograph as something private,[74] thus securing constitutional protection against warrant-less searches.[75]

---

[74] *See* Hodge, *supra* note 2, at 106.

[75] *See Katz*, 389 U.S. at 351.

In fact, that exact conclusion seems follows naturally given the way many people interact in online communities. Many users limit their profiles,[76] carefully choose which "friends"[77] and networks to add, and meticulously de-tag themselves from posted photographs.[78] Such actions designed to limit and restrict the availability of information to certain groups inherently display a user's intent to secure privacy, and it takes no great leap of logic to assume that users, having taken such actions, do in fact expect that such privacy exists.[79] Furthermore, these precautions to protect and ensure privacy, though taken in an arguably public medium, engender a collective understanding by community members of the function they serve, strengthening the privacy-protecting user's basis for a subjective expectation of privacy.

What complicates the scenario for current purposes is the fact that any given user can post photographs of *other* people.[80] Thus, while a subjective expectation of privacy in a photograph can be hypothesized, the *Katz* inquiry into whether the subject has

---

[76] *See* Hodge, *supra* note 2, at 110–11.

[77] *See* Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, Tech Support, at 6 (reporting one user's "picky" approach to establishing friends), *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html (last visited Nov. 14, 2008).

[78] *See id.* ("De-tagging removing—your name from a Facebook photo—has become an image-saving step"). As one student put it, "[t]he event happens, pictures are up within 12 hours, and within another 12 hours people are de-tagging." *Id.*

[79] *See* Hodge, *supra* note 2, at 110 (noting that it is questionable whether limiting profiles via privacy settings "will overcome the presumption that by posting information on a profile, users cannot actually expect privacy because they are sharing personal information in a style much like a bulletin board or a yearbook").

[80] Jim Saska, *Facebook—the fall of privacy*, THE DAILY PENNSYLVANIAN, Mar. 31, 2008, http://media.www.dailypennsylvanian.com/media/storage/paper882/news/2008/03/31/Opinion/Jim-Saksa.Facebook.The.Fall.Of.Privacy-3292188.shtml (describing the unsettling situation where a student in the library observed a complete stranger viewing photos of him that a friend had posted) (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

"knowingly expose[d] [the photo] to the public"[81] does not apply neatly to the context of personal information being provided by *someone else*. Here, both the content of the photograph and the identity of the uploader become key considerations for the *Katz* analysis. When a photograph's content reveals something blatant and obvious or when the activity is being performed openly and notoriously, it is easy to see how a subjective expectation of privacy is not likely to attach. However, when the content of the photograph is of a murky, questionable nature, or when the activity is being performed in a clearly personal setting, a person may logically hold a subjective expectation of privacy.

Furthermore, these expectations of privacy may operate at different levels, owing to the varying levels of publicity which are possible. To begin with, the subject of a highly private or intimate photograph may never expect that such a photograph would be uploaded onto a social networking website. Alternatively, a pictured individual may expect the posting of a photograph, while at the same time expecting that certain protections will reliably secure his or her privacy interests. These protections could come in concrete forms, such as the uploader posting photographs without identifying the subject's name, the absence of link-creating tags, or through the varying degrees of privacy available to online photograph albums.[82] However, the protections could also be more general. For example, before determining whether a particular photo deserves an expectation of privacy (which is, most of the time, not a fully conscious determination) the pictured individual may consider the prototypical online behavior of the uploader. This consideration could involve whether the uploader generally posts a lot of photographs, tags every pictured individual or just certain friends they know would approve of being tagged, or makes lots of attention-drawing comments. Additionally, the pictured individual would likely factor in the general composition of the audience who will see the photographs (who is the uploader friends with?) in formulating whether to place a privacy

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

[82] *See* Guernsey, *supra* note 77 (citing Educause study showing "45 percent of students who use social-networking sites put 'a lot' of restrictions on who can see their profile; 41 percent put 'some' ").

expectation in the photograph. Regardless of whether the protections are concrete or more general, the photograph subject may still subjectively expect the photograph to remain private, even though he or she was not responsible for posting the photograph to the online social network.

B. *Objectively Reasonable Expectation of Privacy*

Subjective privacy expectations of a given photograph subject are not enough to protect that photograph from search and seizure. "[T]he police may still take any measure without a warrant to discover . . . information if society is not prepared to recognize an expectation of privacy in that material."[83] The ultimate question thus boils down to this: is society prepared to recognize an expectation of privacy belonging to the subject of a photograph posted to an online social networking site by another user?[84] Traditional notions of what is considered private in cyberspace suggest that courts would answer this question in the negative.[85] However, given the practical realities of the social interactions on networking sites and the reasonable anticipations guiding their users, these notions must be adapted so that this question can be answered affirmatively—at least in certain circumstances.

---

[83] Hodge, *supra* note 2, at 112.

[84] At least one country, Ireland, has enacted or interpreted law to recognize such a privacy expectation. *See Yes, you are a cyber criminal*, THE POST.IE, Nov. 16, 2008, http://www.thepost.ie/post/pages/p/story.aspx-qqqt=TECHNOLOGY-qqqm=nav-qqqid= 37504-qqqx=1.asp ("Suppose you're out and about and see a child frolicking in a fountain. Or perhaps a homeless man painting a mural. Or even a newly-married couple kissing. It is against data protection law to upload those images to your . . . Facebook . . . account[]. Those images are the personal data property of the subjects involved and explicit permission must be attained prior to uploading them.") (last visited Nov. 16, 2008) (on file with the North Carolina Journal of Law & Technology).

[85] *See* Hodge, *supra* note 2, at 113 (noting "the objective prong is a difficult prong to overcome" in the cyberspace context due to the consistent position of the Supreme Court that a person has no legitimate expectation of privacy in information turned over to a third person).

Finding such an objectively reasonable expectation of privacy requires tossing out the abstract conceptions of cyberspace[86] and the awkward analogies to 20th Century objects and communications that have shaped cyberspace privacy law.[87] If such devices ever did properly frame the issues, they no longer match the reality of today. Instead, new conceptions must emerge to recognize the *electronic lives* that members of society lead today. For example, a traditional argument suggests that simply "[b]y signing on to Facebook or MySpace and providing personal information for others to see, a user is, in effect, not seeking to preserve the information as private, but is instead making a choice to publicize this information for others."[88] But in light of the vast use of online social networks and the type of historically private information readily provided on user profiles,[89] this is not *necessarily* the case. Rather, it seems that society—or at least the growing portion of society comprised by social network users—has in many respects applied traditional privacy expectations to online profile pages and social network users operate accordingly.[90] These users trust their friends, their individual

---

[86] Even the name "cyberspace" has, at least in part, "otherworldly" connotations (suggestive of science fiction, even) that belie the very real role it plays in life today.

[87] *See* Hodge, *supra* note 2, at 101–06.

[88] *Id.* at 106.

[89] One user purports to have photographs on Facebook showing himself urinating in public, wearing women's clothing, and "making out with an ugly girl," along with numerous drinking escapades. Jim Saska, *Facebook — the fall of privacy*, THE DAILY PENNSYLVANIAN, Mar. 31, 2008, http://media.www.dailypennsylvanian.com/media/storage/paper882/news/2008/03/31/Opinion/Jim-Saksa.Facebook.The.Fall.Of.Privacy-3292188.shtml (describing the unsettling situation where a student in the library observed a complete stranger viewing photos of him that a friend had posted) (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

[90] For example, consider the quote of Robyn Backer, who, while a student at Virginia Wesleyan College, described her approach to de-tagging: "If I'm holding something I shouldn't be holding, I'll untag . . . [a]nd if I'm making a particularly ugly face, I'll untag myself. Anything really embarrassing, I'll untag." Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, Tech Support at 6 (reporting one user's "picky" approach to establishing friends), *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html (last visited Nov. 14, 2008). By de-tagging, Backer

monitoring of their networks,[91] their privacy settings[92]—and, through inaction, their government—to keep certain information private.

In this sense, a user's online profile is in many ways similar to a person's home.[93] On its face, or from an anachronistic perspective, such a comparison might seem crude, but close inspection reveals that the analogy provides a nuanced and leveled approach to privacy in a cyberspace life. The two environments provide close parallels with regard to human behavior and expectations in the privacy context.[94] The most pertinent similarities between a home and a user's online profile include: (1) social and legal standards generally require permission for

---

indicates her desire to preserve the "embarrassing" photographs as private and is not publishing the information for others. Furthermore, by not asking the uploader to take the embarrassing photographs down, Backer evidences her expectation that the photographs will remain sufficiently private, despite her knowledge that they remain accessible to certain users (presumably ones she would permit to view them).

[91] Users employ vigilance as a privacy-protection strategy, monitoring what information is being disseminated about them on Facebook to ensure their privacy remains protected. *See id.* (quoting one user's advice: "'Stay on top of it . . . and make sure you know who can see what'").

[92] *See id.* (discussing a user attempt to secure privacy by limiting the viewers of her photo albums to friends only, as well as excluding specific friends or groups of friends from seeing photographs in which she is tagged).

[93] One user termed his Facebook profile "a *comfortable haven* amidst the sprawling, faceless Internet." Kai Stinchcombe, *Facebook Privacy*, THE STANFORD DAILY ONLINE, Sept. 25, 2006, http://daily.stanford.edu/article/2006/9/25/facebookPrivacy (emphasis added) (last visited Nov. 15, 2008) (on file with the North Carolina Journal of Law & Technology).

[94] These privacy expectations with respect to the online social profile were dramatically revealed when Facebook introduced its news-feed feature and experienced fierce and immediate backlash, due largely to the way that feature represented a usurpation of user control over information users considered private. *See* Associated Press, *Facebook feature draws privacy concerns; Backlash over alerts when personal profile pages changed by friends*, MSNBC.COM, Sept. 8, 2006, http://www.msnbc.msn.com/id/14728756/ (on file with the North Carolina Journal of Law & Technology).

entry and inspection;[95] (2) friends and acquaintances can reasonably be deemed to have open invitations[96] while strangers[97] and the government do not;[98] (3) extra mechanisms exist to protect against intruders;[99] and (4) in light of these general assumptions, people willingly bare private facts about their lives, comfortable such facts will not escape such a private space.[100] The fact that some of these private facts may be exposed via the photograph-posting actions of another user is immaterial; the artificial environment of online social communities creates a feeling of sanctity that results in a pattern of user behavior that reflects true expectations of privacy.[101] In other words, online social network

---

[95] At their most basic levels, both entities have a series of "barriers" to the outside world. A home may be protected by gates or fences, an expanse of private property that would require trespassing to cross, as well as lockable entry points. Similarly, gaining access to a social networking profile may require user membership at the outset (analogous to a gated community) as well as further protective hurdles as established by limited-access privacy settings. Additionally, the profile itself is subject to the sole control of its creator, as secured by user-created passwords (similar to the security passwords that may protect a home).

[96] *See* Stinchcombe, *supra* note 93 ("Facebook . . . create[s] a comfortable place where users can feel safe sharing their information" and can control who they share information with).

[97] *See* Kim Hart, *A Flashy Facebook Page, At A Cost To Privacy: Add-Ons to Online Social Profiles Expose Personal Data to Strangers*, WASH. POST, June 12, 2008, at A1 (describing how a typical user views the ability of "20 guys you've never met" to access information from one's profile as something that "should be troubling to people"), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html (last visited Nov. 15, 2008) (on file with the North Carolina Journal of Law & Technology).

[98] *See* John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1235–36 (2007) (raising questions as to the social and legal acceptability of law enforcement officers or government agents simply logging-in to social networking sites, (or more aggressively, posing as pseudo-friends) in order to procure evidence).

[99] *See id.* (speculating whether password protections and profile-access limitations equate to traditional locks, which have been held to confer reasonable expectations of privacy).

[100] *See* Stinchcombe, *supra* note 93 (describing Facebook as "a comfortable, safe place" where information is shared with a "small group" of peers).

[101] *See* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement at 4A, (quoting a college student expressing just this

users expect friends and acquaintances to come in and look around if the door is open[102]—and users trust their friends to keep the things they see to themselves, or at least within a discrete group.[103] Contrastingly, users generally do not contemplate that law enforcement officers would be welcome to make themselves at home without complying with constitutional guidelines.[104] It is precisely this reflection that inspires users to form objectively reasonable privacy expectations in certain circumstances.

Another traditional mechanism that suffers in the social-networking, photograph-posting context is the method for determining when an individual has effectively consented to governmental searches. There are no Fourth Amendment protections when an individual consents to a search, but traditionally such "consent exceptions" have been given broad latitude; thus, "when a person gives information to a third party, the third party is sometimes said to have common authority over the object of the search and can then give 'consent' to its usage by the police."[105] The applications of such a third-party consent

---

sentiment: "Facebook is part of an evolving dialogue . . . . One of the things that's most fascinating about it is how it illuminates the changing nature of public and private identity. This is new ground on every level. What people in positions of power have to realize is that *people my age have a completely different attitude about what is fair game*") (emphasis added), *available at* http://www.nytimes.com/2006/01/08/education/edlife/facebooks.html (last visited Nov. 14, 2008).

[102] This notion is embedded in Facebook's core principles. *See Facebook: Privacy Policy*, http://www.facebook.com/policy.php (emphasizing Facebook's hallmark governing ideal—that "[y]ou should have control over your personal information" and "[y]ou should have access over information others *want to share*") (emphasis added) (last visited Nov. 16, 2008) (on file with the North Carolina Journal of Law & Technology).

[103] *See* Stinchcombe, *supra* note 93 ("We shouldn't always have to be looking over our shoulder to feel comfortable in *our own* online community.") (emphasis added).

[104] *See* Katz v. United States, 389 U.S. 347, 352 (1967) (noting that Fourth Amendment protections apply to various environments, including business offices, friends' apartments, taxicabs, and phone booths).

[105] *See* Hodge, *supra* note 2, at 111. *See also* United States v. Matlock, 415 U.S. 164, 171 (1974) ("consent . . . is not limited to proof that consent was given

exception to a photograph posted on a social networking site does not immediately or rationally follow. Technically, the third party has been given *access* to such information, but it is not clear that the third person has any sort of common authority over the photograph itself. An additional consideration may involve whether the pictured individual is tagged or not; one could view such an action as an express manifestation of consent by the third-party, while the withholding of such identifying information might indicate the third party's unwillingness to give the government permission to access the photo.

Likewise, the "plain view" doctrine, which states that "objects, activities, or statements that [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to [oneself] has been exhibited,"[106] fails in its direct application to photographs posted to online social networks. The most fatal blow to this argument stems from the fact that the photograph's poster, not its subject, is responsible for the exposure. Nevertheless, other weaknesses exist as well. The "plain view" doctrine is predicated on the logic that police (or other government agents) do not have to turn away or hide their eyes to information in their "plain view."[107] However, what is considered "plain view" in social cyberspace is not clear. It would seem logical that the one-step removal from the actual physical setting of the photograph is enough to take it out of "plain view" as the sweeping connotations of that phrase suggest. But even if not, and the information is searchable without a warrant, is the officer only allowed to look at the visible screen? Can he or she click on links? The impossibility of answering these and other unsettled and difficult questions with any sort of consistency or reliability demonstrates the inadequacy of the "plain view" doctrine insofar as it pertains to privacy guarantees that exist in photographs posted to social networking sites. Moreover, the tagged status of the pictured individual could prove vital; perhaps a photograph subject who is tagged would be in the "plain view" of a

---

by the defendant, but may . . . [exist where] permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.").

[106] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[107] *See* Hodge, *supra* note 2, at 108.

perusing law enforcement officer, but an unlabeled, unidentified subject would not and any further searching to identify the person's identity would be unwarranted.

As these traditional search and seizure constructs and formulations inevitably fall victim to such shortfalls, a proper, forward-thinking, practical-reality approach must arise. Such an approach first requires analysis of whether the "communities" created by social networks are themselves deemed public or private.[108] These artificial online groupings can and do share characteristics of both public and private bodies.[109] Additionally, as Internet users become more and more comfortable sharing information online, the distinctions between traditionally private and public information become less definite and clear.[110] While traditional constructs view posting information online as publication to the world, social network users are not irrational in thinking they may have a reasonable privacy expectation when they post limited information, or they intend to limit the information, to select groups of people.[111] Certainly, given a contextual framing of the online group involved (a group of friends, an organization, an entire school, a community, etc.), it is possible to imagine a scenario where sharing information between these discrete users is not properly described as "publication" at all, especially considering that term's historical meaning.[112] Under

---

[108] *See generally* Patricia G. Lange, *Publicly Private and Privately Public: Social Networking on YouTube*, JOURNAL OF COMPUTER-MEDIATED COMMC'N, 13(1), ARTICLE 18 (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/lange.html (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology); Danah Boyd, *Social Networking Sites: Public, Private, or What?"* KNOWLEDGE TREE 13, May 2007, *available at* http://kt.flexiblelearning.net.au/tkt2007/?page_id=28 (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology).

[109] *See generally* Lange, *supra* note 108.

[110] *See* John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1233–36 (2007).

[111] *See* Hodge, *supra* note 2, at 106.

[112] The Supreme Court of the United States has recognized the tendency for privacy considerations to lag behind evolving social constructs fueled by technological advancement, proclaiming that "[t]he law, though jealous of

this theoretical construct, when users post photographs, they do not "publicize" them; they merely allow a known and trusted private group to view them. Eschewing rationalizations based on this publication concept seems appropriate since the intended recipients[113] of information on online social networks differs significantly from the audiences traditionally encompassed by notions of "publication." In this sense, an analogy can be made between social network user actions and the phone communications held private in *Katz*.[114] However, rather than simply involving the phone line transmissions from one individual to another, as in *Katz*, a phone call to a friend where the contents of the call remain private, despite being audible on the other end to a group of common friends, provides a better analogy to the online community situation. If accepted, a revamped construction such as this would go a long way toward establishing the objective reasonableness of privacy expectations in an online world.

On the other hand, as the number and the relative sophistication of Internet users increase, photographs hosted on social networking sites will become even more widely accessible.[115] The logical conclusion is that courts will recognize these photographs as public communication. Undoubtedly, the fact that relevant parties such as law enforcement, school administrators, opposing legal counsel, and even community vigilantes[116] are actively seeking out such material[117] could play a

---

individual privacy, has not kept pace with these advances in scientific knowledge." Berger v. New York, 388 U.S. 41, 49 (1967).

[113] *See* Hodge, *supra* note 2, at 114–15.

[114] *See* Katz v. United States, 389 U.S. 347, 359 (1967).

[115] Or, following the discovery of such a photograph, the photograph could be saved to the viewer's own drive and thus preserved for dissemination via alternative means. Additionally, the photo could be cached on a server and preserved there as well.

[116] Jodie Sinnema, *Facebook vigilantes identify alleged cat killers*, CANWEST NEWS SERVICE, CANADA.COM (VICTORIA TIMES-COLUMNIST), Jan. 7, 2008, *available at* http://www.canada.com/victoriatimescolonist/news/story.html?id=efaf5eb7-2741-4a06-a2ef-cba3dcf18679&k=46162 (last visited Nov. 14, 2008) (on file with the North Carolina Journal of Law & Technology). *see also* Wilson, *supra* note 110, at 1226 ("Some people act as something akin to 'MySpace vigilantes,' using the site to ferret out potential sex abusers").

substantial role in recognizing photographs as public communcation. Still, even the collective awareness that people are possibly searching the Internet to access an implicating photograph does not automatically destroy privacy expectations. It is objectively reasonable to expect that such people will not perform searches unless given a reason or suspicion. Moreover, if a tag is not present, a pictured individual may well have the expectation that no compromise of his or her privacy occurred. Thus, social networking sites in general and user profiles individually, may at different times and with respect to different information be classified as either public or private—and sometimes both simultaneously.

Wrapped up in all these public and private considerations is the actual photograph content, including the setting in which it was taken.[118] Wholly apart from the photograph's eventual posting to an online community, the very content of the photograph may be enough to secure an objectively reasonable privacy expectation. For example, if the photograph detailed highly personal interactions or if a subject only granted consent to be photographed upon express assurances of privacy, society would likely attach a reasonable privacy expectation to such scenarios. These expectations would extend to the unanticipated posting of the photograph online, whether the subject is tagged or not.[119] Related to the photograph's content is its setting; society would be less likely to extend privacy expectations to photographs taken in

---

[117] *See* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, Education Life Supplement at 4A, *available at* http://www.nytimes.com/2006/01/08/education/edlife/facebooks.html (last visited Nov. 14, 2008).

[118] *See* Patricia Sanchez Abril, *Recasting Privacy Torts In A Spaceless World*, 21 HARV. J. L. & TECH. 1, 41–44 (2007) (discussing reasonable expectations as they pertain to possible audiences).

[119] *See* Associated Press, *Naked Photos, E-Mail Get Teens in Trouble*, FOXNEWS.COM, June 5, 2008, *available at* http://www.foxnews.com/story/0,2933,363438,00.html (exposing the wrongness society feels toward private photos being distributed online without authorization, a wrongness that sometimes, in extreme settings, manifests itself in criminal sanctions) (last visited Nov. 17, 2008) (on file with the North Carolina Journal of Law & Technology).

indisputably public places (because no expectation of privacy existed at the time of the photograph), than it would to a photograph taken in a person's home[120] or another intimate setting. Additionally, the number of people captured by the photograph, their relationships to each other, and their subjective expectations regarding the photograph could all influence whether an objectively reasonable privacy expectation exists. Lastly, in deciding the extent to which a photograph's content should influence whether the photograph is objectively considered private or public, the inquiry must focus on the intended audience of the posted photograph.[121]

VI. CONCLUSION

Resolution of Fourth Amendment privacy protections in a social networking world raises some challenging questions: (1) Is it unreasonable to expect privacy in places where such an expectation would have been completely warranted just ten years ago?; (2) Is it fair to ask people to change their behavior in the face of such rapid technological change?; (3) Does the emergence of small, sophisticated, and mobile image-capturing devices paired with the explosion of social networking expose new privacy risks deserving of protection?; and (4) To what extent must law enforcement standards change and adapt in light of these changes? Faced with such a potent, landscape-changing threat to privacy expectations, society must pin its resolution on whether the desired remedy is best found in behavioral modification or in a legal refuge of some sort, perhaps most logically within the confines of the Fourth Amendment.

The simple emergence of social networking sites and the vast dissemination of information that originates from them may have already led to, and may continue to spur, a general reformulating of what is considered "private" in the public conscience generally. As users of these sites become accustomed to seeing, reading,

---

[120] *See Katz*, 389 U.S. at 352 n.8.

[121] *See* Abril, *supra* note 118, at 33 (2007) ("Instead of basing a privacy assessment on its complete seclusion or secrecy, courts should analyze the overall accessibility of the information in question").

sharing, and hearing information that was not traditionally communicated on such a large scale, either out of privacy concerns or simple logistical constraints, it is only natural that a "loosening" or "re-orienting" of the standard for what is truly private could occur. Alternatively, given the increasing possibility for negative consequences resulting from online activities,[122] social network users could come to sense and expect heightened privacy entitlements in certain types or categories of content. Thus, for example, with regard to photographs depicting friends at a small house party, a collective social understanding could emerge that such content, even when posted online, is of the type that the public eye should never see.

In fact, it is quite easy to see how the posting of such photographs (whether or not exposed to prosecutorial forces) could have such reasonable privacy expectations attached that society would deem the photographs protected.[123] Clamoring for some sort of recognition is the seemingly evolving collective sense that some wrong may occur when "'what is whispered in the closet shall be proclaimed from the house-tops,'"[124] or adapted to modern times, when what is photographed in intimacy could be accessible by police laptops. With severe and drastic consequences[125] stemming from such publication, recognition of Fourth Amendment protections inhering in such photos is perhaps overdue.

Current constructs of privacy law do not prove adept at adequately protecting sensible notions of privacy expectations. Something must give. Common sense suggests that drastic behavioral changes are unlikely and that the unabated explosion of social networking websites will likely lead to the development of

---

[122] *See generally* Hass, *supra* note 117.

[123] The privacy interest at issue here might best be conceptualized as that which "enforces socially-accepted codes of civility between members of a community and safeguards intimacy and social ties." Abril, *supra* note 118, at 33.

[124] Samuel D. Warren & Lewis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 195 (1890) (source of internal quotation not cited in original).

[125] *See generally* Hass, *supra* note 117.

even more privacy conflicts.[126] Consequently, it becomes necessary to either reshape how society views privacy in the online social networking context or the constructs themselves must evolve to better envelop those actions which appear in conflict with contemporary notions of privacy entitlements.[127] In the search-and-seizure context, any existing legal protections would seem to find their most logical home in the Fourth Amendment, though the case-by-case determinations required could make such an approach undesirable in practice. Even in the event that such guarantees are not established judicially through the operation—or newfangled recognition—of cyberspace privacy rights, the evolving social dynamics presented by social networking sites recommend the development of some mechanism for protecting privacy online. Such protection could be achieved judicially, legislatively, or via common law tort adaptations, but it seems clear that as society increasingly transfers many of its substantive activities from the concrete physical world to the artificial online world, the law must simultaneously evolve to protect certain privacy entitlements as they exist in their new environments.

---

[126] *See, e.g., id.* (quoting a school official who referred to "Facebook as a land mine.").

[127] *See generally* Abril, *supra* note 118, at 27–47 (positing, in the context of tort law, an interesting and compelling new framework tailored to today's online world for determining whether a disclosure of information is legally protected.