THE FOURTH AMENDMENT AND PRIVACY ISSUES ON THE "NEW" INTERNET: FACEBOOK.COM AND MYSPACE.COM

Matthew J. Hodge*

"One of the things that is most fascinating about [Facebook] 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."[1]

I. INTRODUCTION

In October of 2005, the Penn State University football team won a game against one of its rivals, Ohio State University.[2] This dramatic win caused chaos for thousands of students and fans as they rushed onto the field of play and started a frenzied, post-game near-riot.[3] The police officers at the scene were overwhelmed by this rush of fans and were only able to make two arrests on the day of the game.[4] However, a week later, the police received a tip that several students had posted pictures online of themselves and their friends celebrating on the field after the game.[5] Using this information, campus police identified and referred around fifty alleged offenders to the university's office of judicial affairs.[6] The pictures and offenders' names were found using a social-networking Web site, facebook.com ("Facebook"), which, like its counterpart MySpace.com ("MySpace"), is becoming an increasingly popular and effective tool for law enforcement officers.

The police are using these Web sites to search for evidence in a

---

* Mr. Hodge is a J.D. candidate, Southern Illinois University School of Law, May 2007. He wishes to thank his family and the editorial staff of the Law Journal for their help and support. Mr. Hodge may be reached at mjhodge@illinoisalumni.org.

1. Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, §4A, at 30.
2. Brock Read, *Think Before You Share*, THE CHRON. OF HIGHER EDUC., Jan. 20, 2006, at 38.
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*

variety of offenses. Police at George Washington University, Northern Kentucky University, and the University of Kentucky have charged students with violations for underage drinking and noise violations linked to photos posted online or messages announcing parties.[7] At colleges such as Syracuse University, and additionally at many high schools across the country, administrators are reprimanding students for postings which are critical of professors, teachers, and principals.[8] The Secret Service has even gotten involved, questioning a student at Oklahoma University after he posted on a group titled "Bush Sucks" on Facebook.[9]

Many judges, lawyers, and administrators are unfamiliar with Facebook and MySpace because the Web sites originated less than three years ago. However, in just two years, the popularity of these Web sites has exploded as university students and non-university students under 25 years of age have become very familiar with Facebook and MySpace.[10] In response, the police are becoming more familiar with it every day. According to Business Week, Facebook is the seventh most visited Web site on the Internet, which puts it in the company of giants like Google.com (sixth) and ahead of Amazon.com.[11] The New York Times reports that the average Facebook user will sign on to Facebook six times a day.[12] With the increasing usage of Facebook and MySpace as tools for police searches and prosecution, students and parents around the country are becoming worried about their rights and potential privacy issues on these new and extremely popular Web sites.[13]

This paper will provide a background of the Fourth Amendment issues surrounding the usage of Facebook and MySpace, and discuss the legality of potential searches conducted by police and other law enforcement officials. Section II of this paper will introduce and describe Facebook and MySpace, including the different features, uses,

---

7. *See* Stephanie Perry, *Can Facebook Lead to Your Arrest?*, THE DAILY FREE PRESS - BOSTON UNIV., Jan. 25, 2006; *see also* Hass, *supra* note 1 and Read, *supra* note 2.
8. Nancy Buzcek, *Schools Discipline Students over Internet Content; Four at SU get Probation for "Extreme" Language Critical of Teaching Asst.*, THE POST-STANDARD, February 22, 2006, at A1; *see also* Layshock v. Hermatige School District, 412 F. Supp. 2d 502 (W.D. Penn. 2006).
9. Perry, *supra* note 7.
10. Kevin Coughlin, *The User Friendly Web Site Teens Can't Resist: MySpace.com is Fast Becoming the Online World's Place to Be*, STAR-LEDGER (NEWARK, NJ), December 5, 2005.
11. Steve Rosenbush, *Facebook's on the Block*, BUSINESS WEEK ONLINE, March 28, 2006, *available at* http://www.businessweek.com/technology/content/mar2006/tc20060327_215976.htm.
12. Hass, *supra* note 1.
13. *See generally* Perry, *supra* note 7.

privacy policies, and privacy settings. Section III will then provide a background of Fourth Amendment search and seizure law in the United States and how some of the landmark Supreme Court cases and other relevant decisions might be used in determining Fourth Amendment rights when dealing with Facebook and MySpace profiles. Section IV will apply some of these Fourth Amendment holdings and compare these decisions to how a court would analyze police searches using profiles on the Web sites of Facebook and MySpace. Section V will then discuss whether the privacy policies of Facebook or MySpace may have any additional impact on an expectation of privacy. Section VI will finally conclude with a suggestion on where courts should draw the line between the need to protect individual privacy and the desire not to hinder effective police investigations.

II. WHAT ARE FACEBOOK AND MYSPACE AND HOW DO THEY WORK?

This section will first layout some of the important functions of Facebook and MySpace and discuss how they are used in subsection A. Then, subsection B will cover the privacy policies of Facebook and MySpace, which users must accept upon creating a profile. Subsection C will then discuss the privacy settings that a user is allowed to change, once they have created a profile, in order to further protect the information they release.

A. Some of the Functions of Facebook and MySpace

Facebook and MySpace are typically referred to as social networking sites or friend sites. Facebook was created by two Harvard students in 2004 because they "wanted to animate the black-and-white thumbnail photos of freshman directories."[14] Users of Facebook and MySpace, in addition to posting a photo, can create online profiles, where they can list contact information, school information, personal information, and can even post additional photo albums or diaries.[15] Besides creating profiles and posting information, Facebook and MySpace users can also compile lists of their friends, post public

14. Hass, *supra* note 1.
15. *Id.*

comments on friends' profiles, and send private messages to other users. They can, additionally, create groups of people with similar interests such as "Cubs fans stuck in Cardinal territory" or announce events and invite people to their events. These Web sites also have search functions, which allow users to look up other users by name.

Facebook, at one point, limited the ability to create a profile to only persons with ".edu" email addresses at universities which were approved by the administrators of Facebook.[16] However, recently, it has opened to everyone.[17] Facebook still has an inherent limitation on profile viewing, by grouping users into networks based on affiliation with a university, high school, region of the country, or company, and only allowing other users within a network to view each others' profiles.[18] MySpace is a similar type of Web site where users can create profiles, but it has no networks or inherent limitations on the viewing of profiles. MySpace is open to any user of the internet, in one large network, and as of March 2006, was the second most visited Web site on the Internet behind only Yahoo.com.[19]

B. Privacy Policies

When users register for Facebook or MySpace, they must agree to the Web site's terms of service and privacy policies in order to form a profile and use the Web site. Among others, these terms include how and when the Web sites may collect information from a user's profile and computer, how the Web sites track a user's usage, and how they use the information collected from a user's profile.[20] Additionally, these privacy policies describe when other users can view your profile and when and how the Web sites can disclose information to a third party.[21] The privacy policies are mandatory and must be accepted by a user attempting to register for the Web sites.[22]

---

16. Jennifer Duffy, *Students Respond to Facebook Changes*, ARIZONA DAILY STAR, Sept. 28, 2006.
17. *Id.*
18. *See* www.facebook.com/privacy.php, last visited Sept. 28, 2006.
19. Rosenbush, *supra* note 11.
20. *See* www.myspace.com/Modules/Common/Pages/Privacy.aspx, last visited Sept. 28, 2006 and *supra* note 18.
21. *Id.*
22. For example, "By using or accessing Facebook, you are accepting the practices described in this Privacy Policy." *See supra* note 18.

C. Privacy Settings

While both Facebook and MySpace require users to sign agreements allowing the use of some of their information by administrators, the sites give users the right to set their own privacy settings with regards to other users.[23] Facebook's default settings allow for profiles to only be viewed by registered users of the same network. Users can allow persons from other networks to see their profiles on the default settings by accepting them as "friends." On Facebook, users can compile lists of their "friends" by searching through the database and adding people they know to their friend lists. When a user wants to add a friend, Facebook sends a message to the friend which asks whether this person will accept the requesting user as their friend. If the requested friend accepts, the two new "friends" will be allowed to view each other's profiles. If the friend rejects, neither will be allowed to view the other's profiles. However, if desired, Facebook's privacy settings allow users to change the default settings to limit the viewing of their profiles, or certain aspects of their profiles, to *only* those accepted as their "friends." When users take this extra step, they ensure that only persons whom they accept as friends will be allowed to view their profiles.

MySpace, as a default, allows all other registered users to view a person's profile. However, just like Facebook, users are allowed to change their settings so that only their friends can see their profiles.[24] Many students and young people do not take the time to change their default settings and still believe that the information they post on Facebook or MySpace is private or should be considered private.[25] In sections III and IV, this paper will discuss whether a court might recognize as reasonable this hoped-for privacy in the profiles or messages sent on Facebook and MySpace.

III. BACKGROUND OF FOURTH AMENDMENT SEARCHES

This section will present a background of important Fourth Amendment jurisprudence beginning with discussion of the *Katz* test in subsection A.

---

23. All of the procedures described in this paragraph can be found under *privacy* settings on Facebook, *supra* note 18.
24. MySpace, *supra* note 20.
25. Read, *supra* note 2.

Subsection B will set out how courts analogize the traditional *Katz* test and its progeny when comparing these decisions to cyberspace privacy inquiries. Subsection C will describe two of the more famous Fourth Amendment decisions which will be most relevant as analogies for searches using Facebook and MySpace, and subsection D will lay out how a background of some of the more relevant decisions by lower courts with regards to cyberspace communications.

A. The Katz "Reasonableness Standard"

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.[26]

Prior to 1967, the Supreme Court interpreted this amendment literally, so the Fourth Amendment was not violated as long as there was no official search of a person, or his tangible, material effects.[27] In *Olmstead v. United States*, a divided Court held police wiretapping did not constitute an illegal search under the Fourth Amendment.[28] Justice Brandeis wrote a famous dissent where he argued a literal reading of the Fourth Amendment failed to recognize changing societal conditions.[29]

In 1967, almost forty years after *Olmstead*, the view expressed by Justice Brandeis won a majority of the Court in *Katz v. United States*.[30] *Katz* was another wiretapping case, but this time the Court decided to abandon the literal reading of the Fourth Amendment applied in *Olmstead*, in favor of a new two-step approach to the reasonableness of a search or seizure.[31] The majority in *Katz* agreed that "the Fourth Amendment protects people, not places."[32] However, it was Justice

---

26. U.S. Const. amend IV.
27. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).
28. *See id.*
29. *Id.* at 472–73 ("Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.") *Id* at 472 (Brandeis, J., dissenting).
30. 389 U.S. 347 (1967).
31. *Id.*
32. *Id* at 351.

Harlan's concurring opinion and later cases confirming this opinion which developed the two-step reasonableness standard for Fourth Amendment searches or seizures.[33] Justice Harlan recognized "there is a twofold requirement, first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[34] In order, then, for a search to trigger Fourth Amendment protection, both subjective and objective questions of reasonableness must be answered in the affirmative.

If both questions are answered in the affirmative, the police must acquire a warrant, with its corresponding probable cause requirement, to search the protected area or information in order to not be in violation of the Fourth Amendment. There are, however, exceptions to the warrant requirement, where a person can maintain an expectation of privacy, but the police may still search without a warrant. For example, the police do not need warrants to search while in "hot pursuit,"[35] in performing a protective sweep of a car,[36] or to search a person incident to a lawful arrest.[37]

B. Analogizing Traditional Fourth Amendment Doctrine to Cyberspace

The determination of subjective reasonableness is considered to be an empirical question which fact finders decide using the evidence from each individual case.[38] On the other hand, when courts perform an inquiry into the objective reasonableness of an expectation of privacy, they generally defer to precedents from previous rulings. However, the Supreme Court has yet to voice its opinion on Fourth Amendment privacy in cyberspace, so courts, in performing the objective inquiry, generally have had to draw analogies to previous non-cyberspace rulings.[39] The extent of an expectation of privacy in

---

33. *Id.* at 361; *see also* California v. Ciraolo, 476 U.S. 207, 211 (1986) ("The touchstone of Fourth Amendment analysis is [Harlan's concurrence in *Katz*].").
34. *Katz*, 389 U.S. at 361.
35. Warden v. Hayden, 387 U.S. 294, 310 (1967).
36. United States v. Ross, 456 U.S. 798, 809 (1982).
37. United States v. Robinson, 414 U.S. 218, 234 (1973).
38. *See* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1597 (May 1997).
39. *Id.*

cyberspace, and how closely this expectation would resemble non-cyberspace precedents, has been debated by many commentators and courts. Most of the courts recognize there should be some protection, for instance: "[t]he government may not simply throw up its hands and err on the side of liberally granting its employees access to a wide range of data with the effect of losing the Fourth Amendment somewhere in cyberspace."[40] However, while recognizing a privacy expectation, some courts are hesitant to apply traditional non-cyberspace rulings, stating,

> [t]he advent of the electronic age and . . . the development of desktop 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.[41]

Other courts have felt more compelled to apply the traditional constitutional doctrine that developed after *Katz*.[42]

Cyberspace in general has been difficult for courts to analogize to traditional *Katz* doctrine.[43] Several commentators have put efforts into describing potential analogies between traditional non-cyberspace rulings and compared them to cyberspace communications.[44] In one instance, a commentator compared an e-mail to a parcel of sealed first-class mail and contrasted it with another comparison to a postcard.[45] For any cyberspace inquiry, then, it would be important to determine how to analogize cyberspace situations and communications as the ensuing results may be drastically different in the same fact situation because of differing precedents in tangible communications or situations. For instance, if a court determines that e-mails are, in most aspects, like traditional sealed first-class mail, a person would retain a

---

40. National Treasury Employees Union v. United States Customs Serv., 307 U.S. App. D.C. 173, 184 (D.C. Cir. 1994).
41. United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).
42. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (D. Va. 1999) ("So long as the risk analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology.").
43. *Id* ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").
44. *See* Note *supra* note 38.
45. *Id.*

reasonable expectation of privacy.[46] However, if a court determines that e-mails are like the commentator's other analogy–postcards–the expectation may likely be unreasonable.[47]

C. Relevant Supreme Court Decisions for Analogizing Cyberspace Communications

1. Smith v. Maryland [48]

In *Smith*, the Supreme Court held that the defendant has no subjective expectation of privacy in a search conducted by a pen register.[49] A pen register is a device installed by the telephone company which can track the phone numbers of all calls outgoing from a person's house.[50] The Court refused to recognize an expectation of privacy, stating "all telephone users realize they must 'convey' phone numbers to the telephone company" because they see a list of their long distance calls on their monthly bills.[51] Additionally, the Court held "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as reasonable.'"[52] The Court, however, distinguished this holding from reasonable expectation granted in *Katz* by stating that pen registers do not "acquire the *contents* of communications."[53] Part of the reasoning for this contrary holding in *Smith* came from a line of cases which included *United States v. Miller*,[54] in which Justice Blackmun wrote, "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[55]

2. United States v. Miller[56]

---

46. *See Ex Parte* Jackson, 96 U.S. 727, 733 (1877).
47. *See* Smith v. State, 389 A.2d 858, 873 (Md. 1978) (Cole, J., dissenting)(noting expectation of privacy in a postcard would be unreasonable).
48. 442 U.S. 735 (1979).
49. *Id.* at 742.
50. *Id.* at 736.
51. *Id.* at 742.
52. *Id.* at 743(citing Katz v. United States, 389 U.S. at 361).
53. *Id.* at 741(emphasis in original).
54. 425 U.S. 435 (1976).
55. *Smith*, 442 U.S. at 743–44.
56. 425 U.S. 435 (1976).

In *Miller*, the Court found no protected Fourth Amendment interest in a person's bank records.[57] The Court stated "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[58] The Court went on to reason that "respondent can assert neither ownership nor possession" and therefore the bank records were not "private papers."[59] The Court further noted "[a person] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[60]

The Supreme Court had weighed in through *Smith* and *Miller*, that objectively, society was not prepared to or would not recognize an expectation of privacy in either bank records or phone numbers picked up by pen registers. The Court hinted that a person's voluntary actions could work to destroy an expectation of privacy. However, Congress, acting as the voice of society, later enacted legislation partly superseding the decisions of *Smith* and *Miller*.[61] In addition, many state courts have adopted a broader view of privacy rights and have rejected the holdings of *Smith* and *Miller* when interpreting their own constitutions.[62] These actions, taken soon after the Supreme Court decisions, show society's willingness to broaden the expectation of privacy, at least in bank records and phone numbers.

D. Lower Courts' Limited Rulings on Cyberspace Communications

The Court of Appeals for the Armed Forces, in *United States v. Maxwell*,[63] determined that there should be a limited expectation of privacy in some e–mails.[64] In this case, a concerned citizen contacted

---

57. *Id.* at 440.
58. *Id.* at 442.
59. *Id.* at 440.
60. *Id.* at 443.
61. *See* 12 U.S.C. § 3405 (2006)(a Government authority may only obtain financial records if the records are relevant to a "legitimate law enforcement inquiry" and if a copy of the summons has been served on the customer); *see also* 18 U.S.C. § 3121 (2006)(most pen registers may only be used with a court order).
62. *See* Frances A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge for Traditional Legal Doctrine*, 24 RUTGERS COMPUTER & TECH. L. J. 305, 330–31 (1998)("There is a parallel between *Miller* and *Smith*: Both cases have been rejected by state courts . . .").
63. 45 M.J. 406 (C.A.A.F. 1996).
64. *Id.*. at 419.

law enforcement officials about obscene e-mails he was receiving from another individual.[65] The citizen turned over the e-mails to agents, and the agents later contacted America Online (AOL), an internet service provider, for other files related to the individual who sent the e-mails to the concerned citizen.[66] The police conducted a search of the AOL records instead of a search of a private home or computer.[67] The court held, in this instance, that there was a reasonable expectation of privacy in the AOL e-mails.[68]

The court used analogies to traditional Fourth Amendment doctrine, and compared e-mails to first-class mail[69] and telephone calls.[70] Significantly, the court also reasoned that "the fact that an unauthorized 'hacker' might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way."[71] The court was hesitant to allow an expectation of privacy to be diminished or destroyed merely because it was sent through AOL and this service was needed to send the message.[72] The court used AOL's privacy policy as evidence to backup its reasoning because AOL's stated policy was to only disclose subscribers' e-mail if given a court order.[73] It compared messages sent on AOL to the open internet, which the court said had a less secure system, but recognized an expectation of privacy in AOL e-mails, even though "implicit promises or contractual guarantees of privacy by commercial entities do not guarantee a constitutional expectation of privacy."[74]

The court hinted that it might not recognize a reasonable expectation of privacy when an e-mail was "sent out to more and more subscribers" or sent to the public at-large as in a chat room.[75] It finally held that any information turned over by the concerned citizen was fair game, but once the officials wanted to further search the computer files,

---

65. *Id.* at 412.
66. *Id.*
67. *Id.* at 413.
68. *Id.* at 419.
69. The court drew "parallels" to other mediums, stating that "the sender [of first-class mail] can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause." *Id.* at 417.
70. "Similarly, the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation" *Id.* at 418.
71. *Id.*
72. *Id.*
73. *Id.* at 417.
74. *Id.*
75. *Id.* at 419.

they had to obtain a valid warrant.[76] Another military appeals court later confirmed that individuals have a reasonable expectation of privacy in e-mails sent on a government computer and retrieved by law enforcement officials.[77]

Other courts, however, have found no reasonable expectation of privacy in e-mails. In *U.S. v. Charbonneau*[78] the district court stated "an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received."[79] In this case, the e-mails were sent to an undercover police agent who sought to use the e-mails as evidence.[80] The court here cited to *Maxwell*, and noted "[t]he expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and recipient of the e-mail."[81]

The Court of Appeals for the Armed Services again dealt with the issue of a reasonable expectation of privacy in e-mail transmissions in *U.S. v. Monroe*,[82] where, this time, it found an individual lacked a reasonable expectation of privacy in the e-mails sent on the Air Force system, where a specific notice was given that persons logging on to the system consented to monitoring.[83] Courts have also held that individuals have no expectation of privacy in chat rooms[84] and some computer bulletin boards.[85] Because of the infancy of the Web sites of Facebook and MySpace, courts have yet to rule on whether there would be an expectation of privacy on these servers.

IV. IS THERE ANY EXPECTATION OF PRIVACY IN FACEBOOK OR MYSPACE?

This section will discuss first whether there should be a subjective expectation of privacy in a Facebook or MySpace profile in subsection A. General arguments about subjective expectations will be presented first, followed by specific analysis of a default MySpace profile, a default Facebook profile, and a Facebook or MySpace profile with

76. *Id*.
77. *See* United States v. Long, 61 M.J. 539 (N.M.C.C.A. 2005).
78. 979 F. Supp. 1177 (S.D. Ohio 1997).
79. *Id.* at 1184.
80. *Id.* at 1185.
81. *Id.*
82. 52 M.J. 326 (C.A.A.F. 2000).
83. *Id.* at 330.
84. Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001).
85. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

extra privacy settings. Then, in subsection B, this paper will look at some recognized consent exceptions to the warrant requirement and how these would destroy an expectation of privacy. Finally, in subsection C, this paper will debate whether courts would recognize an objective expectation of privacy in a Facebook or MySpace profile.

A. Subjective Expectation of Privacy in a Profile

In applying the *Katz* test for reasonableness, courts first look to whether a person had an actual (subjective) expectation of privacy.[86] This inquiry, in the words of the *Katz* majority, is whether the individual has shown that "he seeks to preserve [something] as private."[87] In *Smith*, the Supreme Court rejected the petitioner's argument that he had a subjective expectation of privacy in the phone numbers he dialed.[88] While the Court admitted "subjective expectations cannot be scientifically gauged," it used law review articles, consumer information pages in telephone books, and evidence logically assumed from everyday telephone use to determine its rejection of a subjective expectation of privacy.[89]

In trying to prove a subjective expectation of privacy in a user's profile, the inherent nature of the action or its everyday use works against any notion of an expectation of privacy. By 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. There is no substantial need to have a profile on Facebook or MySpace in order to engage in other, everyday activities and there are no institutions which require registration and the posting of a profile on one of these Web sites. In fact, there are other cyberspace mediums for the sharing of personal information with others which hold themselves out to be more private, and can be used without any additional cost to a user. In *Maxwell*, the court recognized that "e-mail messages are afforded more privacy than similar messages on the Internet."[90]

---

86. *See supra* text accompanying note 34.
87. *Katz*, 389 U.S. at 351.
88. *See supra* text accompanying notes 49–52.
89. *Smith*, 442 U.S. at 742–43.
90. *Maxwell*, 45 M.J. at 417.

Profiles on Facebook or MySpace, in general, are unlike e-mails in that they are not strictly a person-to-person communication and there is no intention on the part of the user, or assurance inherent in the communication that only the recipient will be able to view the information presented. Facebook or MySpace, in this aspect, would be better compared to a yearbook, directory, or bulletin board. In each of these examples, users are communicating information for more than one person by posting that information on a naturally public platform. The Sixth Circuit recognized that "[u]sers would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[91] In order for users of Facebook or MySpace to prove a subjective expectation of privacy, they must first overcome an inherent assumption that they intend to make their information public. This assumption should not be completely controlling because, as the Supreme Court showed in *Smith*, it uses many different sources of evidence to determine a subjective expectation of privacy.[92]

There are differing privacy policies, settings, and characteristics between MySpace and Facebook. Because of these differences, this paper will specifically analyze other evidence a court might use in three types of profiles below: a default MySpace profile, a default Facebook profile, and a Facebook or MySpace profile limited for viewing to only "friends" (hereinafter "limited profiles").

1. Default MySpace Profiles

On MySpace, a user's profile is available to the public. There are no restrictions on who may view a user's profile or information.[93] Because of the lack of restrictions, any person surfing the web, including a law enforcement official, would be able to view this profile by merely creating their own profile on MySpace. In addition, there is a search feature on MySpace, which allows a person to type in a user's name and facilitates a search for a user's profile. By posting information which is knowingly available to the general public, MySpace users, through their default profiles, create what would seemingly be a perfect example of "materials intended for publication

91. *Guest*, 255 F.3d at 333.
92. *See supra* text accompanying note 89.
93. *See supra* note 20 (the Web site states that your profile is intended for public viewing in order to facilitate user interaction in the social networking community).

or posting."[94]

Given these conditions, a user could only try to argue that a MySpace profile is not public knowledge, and that it is so obscure as to force the police to go searching for the profile.[95] This obscurity and the fact that the police need a password to sign on to MySpace, could be argued to deem some expectation of a private area. A user may also argue that the privacy policy of MySpace protects them against searches by the police. This argument will be discussed in detail below in section V.

However, even if a person could show an actual expectation of privacy, an exception to the warrant requirement of the Fourth Amendment applies when an object is in "plain view."[96] Within the plain view doctrine, the police can view open fields even if they are privately owned,[97] they can peer inside a barn from an open field,[98] or they can view items inside a house if they are there lawfully.[99] Generally speaking, an officer who is legitimately in a location may use any evidence which is discovered in plain view.[100] The Supreme Court has held that police cannot reasonably be expected to avert their eyes from evidence of wrongdoing that can be observed by members of the public.[101] Because the police may lawfully search on the internet, and any person, including law enforcement officials, may sign up for an account on MySpace, all information on a user's profile would most likely be in plain view and therefore no Fourth Amendment search would occur. At least one court has found, in a similar situation, that there is no reasonable expectation of privacy in information on a website which is released to the public.[102]

---

94. *See supra* note 91.
95. In spying on toilet stalls, a private place in a public area, a California court held "[a]uthority of police officers . . . will not be sustained on the theory that if they watch enough people long enough some malum prohibitum acts will eventually be discovered." *See* Bielicki v. Superior Court, 57 Cal. 2d 602 (Cal. 1962); *But see* People v. Heath, 266 Cal. App. 2d 754 (Cal. Ct. App. 1968) (where a toilet stall without a door was held to not be a protected area).
96. Under the plain view doctrine, "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." *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
97. Oliver v. United States, 466 U.S. 170, 181 (1984).
98. United States v. Dunn, 480 U.S. 294, 304–05 (1987).
99. Ker v. California, 374 U.S. 23, 43 (1963).
100. Georgia v. Randolph, 126 S. Ct. 1515, 1536–37 (2006).
101. California v. Greenwood, 486 U.S. 35, 41 (1988).
102. *See* J.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 425 (Pa. Commw. Ct. 2000).

2. Default Facebook Profiles

A creator of a Facebook profile, like a MySpace profile, may also have knowingly posted material for the general public to see. The main difference is that the "general public" in this case would consist of only those who can obtain an e-mail address from the same network (by university, location, high school, or company), and thus a profile in the same network. University students are sometimes not aware the police can obtain an ".edu" address,[103] but the more logical assumption is that every student is or should be aware that their university has a police department. A student should be aware that these officers either have or can get ".edu" addresses because university police officers are employees of the university. Users in networks by location should also be aware of the minimal requirements for police to create profiles and, thus, access to viewing others' profiles. Users in the other two types of network, high schools and companies, may have a higher, naturally built-in hurdle for police access to their networks. However, control of e-mail addresses to these networks are held by the administration of the schools and companies. If the administration allows the police to obtain a network e-mail address, it is most likely that a court would consider a default Facebook profile, in any network, to be materials intended for publication or public posting and thus could be viewed by the police.

Again, however, even if a subjective expectation of privacy was found in a Facebook profile, the plain view doctrine may work to destroy that expectation. Once the law enforcement official is registered, he would be legitimately in a location where he could view a person's Facebook profile. A user of Facebook may argue, however, that because of Facebook's design, a user is entitled "at least, to the modicum of privacy its design affords, certainly to the extent that he will not be joined by an uninvited guest or spied upon by probing eyes."[104] However, like the unfortunate e-mailers in *Charbonneau* or *Monroe*, an expectation of privacy would only be as strong as the controls Facebook actually has on allowing access.[105]

---

103. Read, *supra* note 2. ("Facebook appears to be a hermetically sealed community, since only those with college e-mail addresses can join.") The article goes on to describe how students complained because they did not know that administrators could look at the site.

104. Brown v. State, 3 Md. App. 90 (Md. Ct. Spec. App. 1968) (where the police took extra efforts to put his head over a 5 foot 5 inch high door to look in a toilet stall).

105. *See supra* text accompanying notes 78–82.

3. Limited Profiles

On Facebook and MySpace, users are allowed to restrict their privacy settings to only allow those who they accept as "friends" to view their profile. This setting is not the default, but instead, a user must actively change the settings to restrict access. This active step may show the intent required to keep the posted information private. This action to protect could be considered the equivalent of installing a lock on a door[106] or setting a passcode or password for entrance to an area.[107] It is questionable, however, whether taking this step 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.

This problem is quite unique in that a user is, on one hand, taking measures to share information with a group of selected people which could be shared individually and stored privately in the form of an e-mail. On the other hand, the user has taken an active step which Facebook and MySpace allow, and even encourage, to ensure approximately the same amount of privacy from intrusion.[108] If a person wanted to share information with a group of friends, he could send a "mass" e-mail[109] to all of his selected friends. This information could only be viewed by his friends and only by entering their passwords and retrieving the information from their e-mail inboxes. In the same way, a person could share information with a group of friends by posting it on Facebook. This information, like the mass e-mail, could only be viewed by his friends and only by entering their passwords and signing onto Facebook. In this way, it is hard to imagine a different outcome in determining whether there is a

106. United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a doublelocked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause.").

107. *See* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995) (arguing that a password is one of the protections a computer user can rely upon to establish an expectation of privacy).

108. *See supra* notes 18 and 20.

109. A "mass" e-mail is an e-mail where the subject matter is identical and is sent out at the same time to more than one selected e-mail address.

subjective expectation of privacy between e-mails, at least mass e-mails, and restricted profiles.[110]

Even if a Facebook or MySpace profile were compared to a non-cyberspace object such as a bulletin board, the subjective expectation of privacy in this third, limited type of profile could be recognized. If a default MySpace profile is like a bulletin board, posted for all to see, there are no restraints stopping the police from viewing it. A default Facebook profile would then be like a bulletin board posted in a university building or at company headquarters, where if police were granted access to the building, they could, of course, view the posting. The third, restricted profile, would then be like a bulletin board posted in a building where access is only granted by the user. The user would expect privacy from police viewing of his bulletin board posting because he would be in charge of granting access to the building. This should be enough to show an actual, subjective expectation of privacy, and therefore, a search violating the Fourth Amendment unless, of course, the police could gain access to the information through one of the other recognized exceptions to the warrant requirement, or society was not willing to recognize the privacy of the communication as reasonable.

B. Consent Exceptions

One of the exceptions to the warrant requirement is when a person gives consent to search a protected area. The Supreme Court has stated "[i]t is equally well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent."[111] This exception applies anytime a person voluntarily gives information, or the consent to search, to the police, even if the police officer is working undercover.[112] A person assumes the risk that the person they are speaking to is an undercover agent when he gives consent to access a

---

110. Courts have, however, hinted that an e-mail forwarded to more than one person would not be private. *See Maxwell*, 45 M.J. at 412 ("Messages sent to the public at large in e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy."). A mass e-mail is not, though, forwarded from correspondent to correspondent, but instead is delivered once to many correspondents.

111. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

112. *See* Hoffa v. United States, 385 U.S. 293 (1966).

protected area or information.[113] In terms of a Facebook profile, if a user accepts a person as a "friend" who turns out to be a police officer, the user's expectation of privacy in the material viewed would be destroyed.

As a part of the consent exception, 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.[114] Under this exception, when persons turn over "joint access or control" to information or the area to be searched, they again assume the risk that the third party will disclose the information or object to the police.[115] There is not a concrete definition as to how much "joint access or control" is required to allow another person to consent to a search.[116] However, in regards to the restricted profile, if a user's "friends" were to allow the police to sign on to Facebook using one of their passwords, the expectation of privacy would certainly be destroyed, as the user has turned over access to his information to the "friend." Though it is unclear whether the Facebook administrators would have such "joint access or control" so as to consent to a search, most Facebook users probably subjectively expect that administrators cannot or should not view their profile which they have attempted to keep private. This consent exception, however, may hinge on whether, through the Web site's privacy policy, a user gave up the expectation of privacy. This subject will be discussed in Section V. If no warrant exceptions apply and if a court finds a user to have a subjective expectation of privacy in a profile on Facebook or MySpace, this expectation still must be "one that society is prepared to recognize as reasonable" in order to be protected by the Fourth Amendment.[117]

C. Objective Expectation of Privacy in a Profile

The objective prong of the *Katz* test requires more than a person's

---

113. *Id.*
114. *See* United States v. Matlock, 415 U.S. 164 (1974).
115. *Id.*
116. *See* Stoner v. California, 376 U.S. 483 (1964) (hotel clerk could not consent to search); Chapman v. United States, 365 U.S. 610 (1961) (landlord could not consent to search); *but see* Frazier v. Cupp, 394 U.S. 731 (1969) (co-user of duffle bag could consent to search even though he only had permission to use one compartment).
117. *Katz*, 389 U.S. at 361.

mere expectation that his behavior is protected.[118] Thus, even if a user sets his privacy settings on Facebook to allow only his "friends" to view his profile, the police may still take any measure without a warrant to discover the information if society is not prepared to recognize an expectation of privacy in that material. In determining an objectively reasonable expectation of privacy in an area not previously ruled on, courts tend to rely on analogies to other, similar areas from prior rulings.[119] For discussion of the objective prong of the *Katz* test, this paper will concentrate on only the limited profile, as this option has the best chance of surviving the subjective prong.

1. Disclosure as an Automatic Destruction of an Objective Expectation

When creating a profile on Facebook, a user creates and stores information on a central computer owned by the Facebook administrators and can access this stored information and change it through the use of a password. The user then can limit access to the information to only "friends" he approves. As previously discussed, it would fall under a clear warrant exception that if these friends consent to allowing the police to see the information, then an expectation of privacy is destroyed. However, if no friends consent, the question remains whether a user has automatically given up an expectation of privacy merely by turning over the information for storage by Facebook or by allowing friends to view it.

In cyberspace, the objective prong is a difficult prong to overcome because the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information turned over to a third person."[120] This statement seems to suggest that once a person discloses any information to any third person, the expectation of privacy is destroyed. However, the rule cannot be this simple, as disclosure to another person does not *automatically* destroy an expectation of privacy.[121] For instance, in *Katz* itself, the defendant gave information in a telephone conversation to another person, yet the

118. *Id.*
119. *See* Note, *supra* note 38.
120. *Smith*, 442 U.S. at 743–44; *see also* Navarro, Francisco J., *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 ALBANY L. J. SCI & TECH. 245, 251–52 (2003).
121. For a discussion of this argument *see* Reetz, C. Ryan, *Warrant Requirement for Searches of Computerized Information*, 67 B.U. L. REV. 179 (1987).

court held there was still an expectation of privacy.[122] The expectation of privacy may depend on when, and how, the police intervene and perform the search. Also, it would be important to determine to what a limited profile is most likely to be compared, and some of the factors involved in the determination of whether disclosure to a third party would destroy an objective expectation of privacy. If a limited Facebook profile is found to be more like a disclosure to a third party such as those in *Smith* or *Miller*, then a user would not have an objective expectation of privacy. However, if a limited Facebook profile were to be found to be more like the disclosure in *Katz*, then there may be an objective expectation of privacy, and thus Fourth Amendment protection.

2. Legitimate Business Purposes

One of the factors that separate the disclosures in *Smith* and *Miller* from the disclosure in *Katz* or other findings of an expectation of privacy was the intended use by the third party with the disclosed information. In *Miller*, the Court found the bank legitimately used the records, they were the property of the bank, and the bank had control and access to the records.[123] In *Smith*, the Court also realized that the phone company must use phone numbers to keep billing records and for other legitimate purposes.[124] In both cases, the disputed information was the records of the business used for business purposes. Because the businesses used the information for legitimate purposes, both companies had an element resembling "joint access or control" over the information. The Supreme Court held in these situations that this disclosure ruined an expectation of privacy.

In *Katz*, the phone company had access to the call, could listen in, and could even memorialize the conversation through a tape recording. While not discussing this aspect specifically, language from the decision hinted that it would have been unlikely the Court would have found a legitimate business purpose for such eavesdropping.[125] Another example like the one in *Katz* is the delivery of mail. A person knowingly releases information in the form of a sealed letter to the post

122. *Katz*, 389 U.S. at 352.
123. *Miller*, 425 U.S. 435.
124. *Smith*, 442 U.S. at 742.
125. *Katz*, 389 U.S. at 361 ("one who . . . pays the toll that permits him to place a call is surely entitled to assume that his conversation is not being intercepted.")(Harlan, J., concurring).

office to deliver it, but the post office would most likely have no legitimate business purpose to open every letter and arbitrarily view the enclosed information.[126] It would seem, then, that one aspect that distinguishes *Katz* or a sealed letter from *Smith* and *Miller* would be whether the third party has a legitimate business purpose in using the disclosed information.

3. Intended Recipient

Secondly, in *Miller*, there were only two parties; the defendant and the bank. The defendant had to turn over the information directly to the bank and clearly intended for the bank to use this information in its everyday business use. In *Smith*, however, there were three parties: the defendant, the recipient of the call, and the phone company, which necessarily got the information in order to connect the other parties. In part of its reasoning, the Court held "all telephone users realize they must 'convey' phone numbers to the telephone company."[127] Thus, it could be reasoned that a person intends to give the phone company the number dialed. In fact, the phone company could not connect the call and perform its duties unless a person conveys this number. Therefore, a phone company could be considered the intended recipient of the phone numbers.

Once an operator receives the phone number and connects the caller and the receiver of the call, a person no longer intends for the operator or the phone company to receive the contents of the call. Thus, it could be said that in a situation like *Katz*, the phone company would not be the intended recipient of the spoken information of a phone call. In addition, when a person sends a sealed letter, she does not intend for the mailman to receive the contents of the letter. The only information a person intends for use by the mailman would be the address written on the outside of the letter. Therefore, another possible factor in distinguishing *Katz* or a sealed letter from *Smith* and *Miller* would be whether the disclosure which would purport to destroy an expectation of privacy was to an intended recipient.

---

126. *See* United States v. Young, 153 F.3d 1079, 1080–81 (9th Cir. 1998)(court stated that FedEx had a legitimate business purpose to inspect packages); *but see* Illinois v. Andreas, 463 U.S. 765, 769 (1983)(noting that "sheer volume prevents systematic inspection of all or even a large percentage of the cargo").

127. *See supra* text accompanying note 51.

4. Memorialization

Finally, in *Miller*, the bank routinely memorialized the information in question, bank records, for easy retrieval by its employees and as a necessary aspect of its business use. In *Smith*, the phone company also routinely memorialized phone numbers called, and this memorialization was evidenced by the phone bill sent out each month.[128] However, in *Katz*, all phone calls were not routinely memorialized by use of a tape recording by the phone company. Additionally, with a sealed letter, the post office has no means, nor does it attempt, to open all letters, scan and copy the contents, and then send the letter on its way. Thus, if a person knows that he is disclosing information to a party which has the means to memorialize the information and routinely does save this information, a court may consider this as a determining factor in whether a person has an objectively reasonable expectation of privacy.

5. Application to a Limited Profile

In regards to a limited profile, a user voluntarily turns over information to the administrators of Facebook or MySpace to store (memorialize) the information. It is routine for the Web site administrators to store this information. In fact, it must be done as a part of the business to enable a user to access the information with a password at a later time. Therefore, with regards to routine memorialization, a limited profile would most resemble the *Smith/Miller* holdings and would lean towards a finding of no reasonable expectation of privacy.

A second distinction may be the intended recipient. Users of Facebook or MySpace, when creating profiles and limiting access to only their friends, could argue that they intend to exclude the administrators of Facebook or MySpace from viewing their profiles. They would argue that their friends are the intended recipients of the information and that the administrators and the central computers are merely the medium for getting that information to their friends. It would be argued that most, if not all, users would not sign up for Facebook or MySpace merely to give information to the administrators for their use. Instead, users sign up to connect to friends and give these

128. *See supra* text accompanying note 51.

friends their information. Therefore, it is likely that a limited profile would be more like a phone call or a sealed letter in this aspect. The disclosure to a third party was not to the intended recipient, but only as a necessary medium, and a court may recognize an expectation of privacy.

In determining whether there is a legitimate business practice for the administrators of Facebook or MySpace to have access to view a person's limited profile, the nature of the transaction should first be considered. In setting up a profile, a user of Facebook or MySpace obtains storage space on a central computer which he and his selected friends can access at will. In return, Facebook and MySpace receive hits on their Web sites and compile a large group of users that marketers can reach. This allows Facebook or MySpace to sell space on its Web site to advertisers. In order to effectively advertise, marketers want to know that their advertisements are reaching the correct audience, or target market, who have specific characteristics and traits. In order to better sell advertising space, then, Facebook collects information about the users of its Web site by viewing and recording information in their profiles in order to present a target market to advertisers.[129] A court may consider this business practice to be legitimate and therefore more like the facts in *Smith* and *Miller*.

Not all potential legitimate business practices, however, should be determined to destroy an expectation of privacy. In *Katz*, one could conceive of a legitimate business purpose, such as monitoring phone calls for quality control. However, this purpose was not enough to destroy an expectation of privacy. Similarly, the post office, as a legitimate business purpose, must be able to open some letters or packages for safety reasons if a bomb or other dangerous material is suspected. The Supreme Court, in discussing just this sort of practice by a private carrier, rejected a finding that this business purpose would circumvent the government authorities' Fourth Amendment

129. As one example: "Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people at a school like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are." *See supra* note 18.

obligations.[130] Therefore, a finding of a legitimate business purpose of collecting marketing statistics should merely be used as one factor in determining an objective expectation of privacy.

The *Maxwell* court used some of these factors when determining the expectation of privacy in e-mails. The court discussed how AOL stored the information, how its business policy was to implicitly promise privacy, and how privacy would depend on "the type of e-mail involved and the intended recipient."[131] Therefore, in discussing the objective reasonableness of an expectation of privacy in a limited profile, a court could determine that the profile is not "intended" to be used by the administrators, but it is memorialized and stored on a central computer. Additionally, while there is a legitimate business purpose for the administrators to use the profile, it is questionable whether this use is legitimate enough to destroy an expectation of privacy merely because a user disclosed the information. To help with this inquiry, a court would need to consider the stated privacy policies of Facebook and MySpace, much like the *Maxwell* court did in its inquiry.

V. HOW THE PRIVACY POLICIES OF FACEBOOK AND MYSPACE MAY AFFECT AN EXPECTATION OF PRIVACY

In *Maxwell*, the court used AOL's privacy policy to help it determine a subjective expectation of privacy exists in e-mails on AOL.[132] More specifically, it stated "it was AOL's practice to guard these 'private communications' and only disclose them to third parties if given a court order."[133] The court used this policy to show that an implicit promise or contractual guarantee by a commercial entity has some bearing on a finding of an expectation of privacy.[134] The privacy policy of Facebook is very similar to AOL's stated policy from *Maxwell.* In particular, Facebook's policy states, "We may be required to disclose user information pursuant to lawful requests, such as

130. "However, [the Supreme Court] has also rejected the proposition that government authorities may rely on broad private searches to circumvent their Fourth Amendment obligations." Warshak v. United States, No. 1:06–cv–357, 2006 U.S. Dist. LEXIS 50076 at *18 (S.D. Ohio 2006)(discussing U.S. v. Jacobsen, 466 U.S. 109, 117–118 (1984).

131. *Maxwell*, 45 M.J. at 419.

132. *Id.*

133. *Id.* at 417.

134. *Id.*

subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards."[135] MySpace's policy is similar, stating "MySpace will not disclose personal information to any third party unless we believe that disclosure is necessary: (1) to conform to legal requirements or to respond to a subpoena, search warrant or other legal process received by MySpace.com, whether or not a response is required by applicable law."[136]

Included, also, in the privacy policies of Facebook and MySpace are the phrases which state that users agree to allow the administrators to use their personal information for advertising or marketing purposes.[137] The user's agreement, as stated earlier, provides additional evidence of a legitimate business purpose for allowing the administrators of Facebook or MySpace to get some information off of a user's profile. Therefore, users are aware that administrators will turn over information to the police when necessary, and have agreed to let the administrators view and compile their information for marketing purposes. This relinquishment of control through the terms of agreement, however, may not be fatal to a finding of a reasonable expectation of privacy.

A recent case out of the Southern District of Ohio provides more guidance on how disclosure to an Internet Service Provider (ISP) affects the expectation of privacy and whether a stated privacy policy has any relevance.[138] The litigation arose because a magistrate judge's order to the ISP to turn over e-mails was "premised upon a showing of less than probable cause."[139] The question in this case was whether it was reasonable to assume that once a person's e-mails are stored on a commercial server, "whatever expectation of privacy the account subscriber may have had in those e-mails [had] already been frustrated."[140] The court agreed with the defendant that in the case of an e-mail, the user actually has more continuing control over the communication, in that he could take it back, than in any other third

135. *See supra* note 18.
136. *See supra* note 20.
137. *See supra* notes 18 and 20.
138. Warshak v. United States, 2006 U.S. Dist. LEXIS 50076 (S.D. Ohio 2006).
139. *Id.*
140. *Id.* at *16.

party carrier setting.[141] This control aspect would necessarily be true of a profile on Facebook or MySpace as well.[142] A user, at any time, can sign on and remove information from their profile. The court then considered and rejected the argument put forth by the United States that through the terms of service, "ISPs and individual account holders routinely both reserve and exercise rights to open, delete, or turn over personal e-mails to law enforcement."[143] The court's rejection of this assertion is the strongest argument for a holding that by agreeing to the terms of the policies of Facebook and MySpace, a person does not automatically relinquish his or her Fourth Amendment rights.

VI. OTHER TANGIBLE COMPARISONS TO A LIMITED FACEBOOK PROFILE

As a final note, and beyond the scope of this paper, courts and practitioners may need to think of a profile on Facebook or MySpace not just in how it communicates information, but also in how it compares to tangible items in order to better understand whether a privacy expectation exists. Because users of Facebook are, in a sense, renting out space on a public computer for their personal use, an appropriate analogy may be to a storage facility or a safety deposit box at a bank. In each case, a person rents a small area in a public facility to store effects or information. The vendors of these areas hold them out to be private, by giving the purchaser a tangible key, or in the case of cyberspace, through a password. In both the case of the safety deposit box and storage area, the vendor/owner may have a legitimate business purpose to have access to the area, but it would not be one which a person would reasonably expect to occur. In both situations, this information, much like the profile with the protection of the extra settings, could be considered to be not in open view, and therefore, be the equivalent of a "closed, opaque container."[144]

---

141. *Id.* at *17.
142. *See supra* text accompanying notes 108–10.
143. *Warshak*, 2006 U.S. Dist. LEXIS 50076 at *18.
144. *See* Robbins v. California, 453 U.S. 420, 426 (1981) (the Court held this placement in a closed, opaque container manifests an objectively reasonable expectation of privacy in that information).

VII. CONCLUSION

Technology and the Internet have evolved to a place unimaginable to people who lived in an era when the *Katz* decision was new. Parents today, in an effort to protect their kids from some information on the Internet, put locks on the content displayed on their computer. These same parents, however, are finding out that their kids are more computer-savvy than them and can easily hack around the locks the parents install. A new generation of citizens are spending more and more of their time online, and establishing their public and private identities through cyberspace mediums. The Supreme Court interpreted the Fourth Amendment through *Katz* and its progeny to provide protection to "people, not places."[145] This was a forward-thinking statement which has helped the Court to interpret the Fourth Amendment to protect citizens from warrantless police searches in ever-changing societal conditions. These statements are very helpful when trying to determine how to apply the Fourth Amendment in cyberspace, which is a tough "place" to define. 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.[146]

Facebook and MySpace are rapidly growing entities, forming a "new" internet, where in just two years, these social-networking Web sites have grown to the seventh and second most visited Web sites on the Internet, respectively. Citizens are learning how to use these sites, and are finding new ways to share information, connect with friends, and meet new people. Courts are starting to recognize that the assumption that merely by turning over information to another, a person loses any expectation of privacy in the information is faulty. A person does not expect that because he invited another into his house yesterday, it can no longer be considered private and can be searched at any time. Likewise, a person does not expect that because he sent an email and it was read by the recipient, it can no longer be considered private and can be retrieved by law enforcement at any time. The consent exceptions allow police a method to access the information.

---

145. *Katz*, 389 U.S. at 351.
146. *See supra* text accompanying note 61.

However, the Internet is not completely private. By creating a profile on Facebook or MySpace, a person is naturally volunteering to show some of their identity and information to others. Whether a person has a reasonable expectation of privacy in this release of information is a difficult determination, but most people are not willing to give up all protection merely by signing online. The police are rapidly evolving their investigative procedures by using Facebook and MySpace in more ways and in a growing number of investigations. With these techniques, it is up to the courts to grow and continue to apply the existing *Katz* doctrine so that the Fourth Amendment does not get lost in cyberspace.