Pace Law Review

Volume 31
Issue 1 *Social Networking and the Law*
Winter 2011

Article 7

January 2011

From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance

Junichi P. Semitsu
University of San Diego School of Law, semitsu@sandiego.edu

From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance

Junichi P. Semitsu*

Abstract

Each month, Facebook's half billion active users disseminate over 30 billion pieces of content. In this complex digital ecosystem, they live a parallel life that, for many, involves more frequent, fulfilling, and compelling communication than any other offline or online forum. But even though Facebook users have privacy options to control who sees what content, this Article concludes that every single one of Facebook's 133 million active users in the United States lack a reasonable expectation of privacy from government surveillance of virtually all of their online activity.

Based on Facebook's own interpretations of federal privacy laws, a warrant is only necessary to compel disclosure of inbox and outbox messages less than 181 days old. Everything else can be obtained with subpoenas that do not even require reasonable suspicion. Accordingly, over the last six years, government agents have "worked the beat" by mining the

* Professor Semitsu teaches at the University of San Diego School of Law and welcomes your feedback at semitsu@sandiego.edu. Once this Article is published, he is very unlikely to accept any friendship requests through Facebook, so please do not be offended if he refuses to give you an opportunity to poke him. He would like to thank the editors of the *Pace Law Review*, USD Law School Dean Kevin Cole, Kirstin Ault, and the following all-star USD Law School students for their invaluable assistance with this Article: Renee Keen, Breehan Carreon, Katherine Carlson, Michael Gilberg, Erik Johnson, and Andrew Gil. He is also grateful to the students in his Fall 2010 Media Law course, who provided some sources and feedback. Finally, he would like to thank his wife and son for their patience.

treasure trove of personal and confidential information on Facebook.

But while Facebook has been justifiably criticized for its weak and shifting privacy rules, this Article demonstrates that even if it adopted the strongest and clearest policies possible, its users would still lack reasonable expectations of privacy under federal law. First, federal courts have failed to properly adapt Fourth Amendment law to the realities of Internet architecture. Since all Facebook content has been knowingly exposed to at least one third party, the Supreme Court's current Fourth Amendment jurisprudence does not clearly stop investigators from being allowed carte blanche to fish through the entire site for incriminating evidence. Second, Congress has failed to meaningfully revise the Electronic Communications Privacy Act (ECPA) for over a quarter century. Even if the ECPA were amended to cover all Facebook content, its lack of a suppression remedy would be one of several things that would keep Facebook a permanent open book. Thus, even when the government lacks reasonable suspicion of criminal activity and the user opts for the strictest privacy controls, Facebook users still cannot expect federal law to stop their "private" content and communications from being used against them.

This Article seeks to bring attention to this problem and rectify it. It examines Facebook's architecture, reveals the ways in which government agencies have investigated crimes on social networking sites, and analyzes how courts have interpreted the Fourth Amendment and the ECPA. The Article concludes with an urgent proposal to revise the ECPA and reinterpret *Katz* before the Facebook generation accepts the Hobson's choice it currently faces: either live life off the grid or accept that using modern communications technologies means the possibility of unwarranted government surveillance.

I. Introduction

"I want everybody here to be careful about what you post on Facebook, because in the YouTube age, whatever you do, it will be pulled up again later somewhere in your life."

- President Barack Obama[1]

Facebook is not just a website. It is a controlled ecosystem that inspires its inhabitants to share personal information and reveal intimate thoughts. It is an evolving digital world that eliminates the limitations of distance, time, technology, and body odor in "real space" to create connections and communities unimaginable in the twentieth century.

Facebook also happens to be the most popular destination on the Internet[2] today.[3] Russian investor Yuri Milner, who owns ten percent of the company, commented that it is "the largest Web site there has ever been, so large that it is not a Web site at all."[4] Fulfilling CEO Mark Zuckerberg's goal to "dominate"[5] online communication, the site, as of September 2010, comprises over 500 million active users,[6] half who log on

---

1. *Obama Warns U.S. Teens of Perils of Facebook*, REUTERS, Sept. 8, 2009, *available at* http://www.reuters.com/article/idUSN0828582220090908.

2. In this Article, I am attempting to consciously use the word "Internet" and avoid the "World Wide Web" or "the web." This is due in part to the fact that Facebook is part of the growing trend to move from the World Wide Web to "semiclosed platforms that use the Internet for transport but not the browser for display." *See* Chris Anderson & Michael Wolff, *The Web is Dead. Long Live the Internet*, WIRED MAGAZINE (Aug. 17, 2010), http://www.wired.com/magazine/2010/08/ff_webrip/all/1. Today, browser content constitutes less than 25 percent of the Internet traffic and is only shrinking further. *Id.*

3. *See* Michael Arrington, *Hitwise says Facebook Most Popular U.S. Site*, TECHCRUNCH (Mar. 15, 2010), http://techcrunch.com/2010/03/15/hitwise-says-facebook-most-popular-u-s-site/.

4. *See* Anderson & Wolff, *supra* note 2.

5. Jose Antonio Vargas, *The Face of Facebook*, NEW YORKER (Sept. 20, 2010), http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas?currentPage=all.

6. If it were a country, Facebook would be the third most populous nation in the world, with a birth rate that would allow it to surpass China and India in just a few years. According to the United Nations, China's population was 1.346 billion and India's was 1.198 billion in 2009. *See* U.N.

daily.[7]

Collectively, this community disseminates more than 30 billion pieces of content per month to audiences chosen by their creators.[8] Its dominance in social media stems from the fact that it has moved beyond its origins as a peephole to pry into others' lives. Today, Facebook has transformed into a simple, one-stop, all-purpose, habit-forming site for everyone from the underage to the golden-aged, neophytes to techies, gamers to political activists, and even pets to corporations.

When its membership expanded, so did its appeal and its potential to effect change and create connections. Facebook has sparked many marriages between strangers,[9] named babies,[10] served as an alibi for the wrongly accused,[11] united long-lost relatives,[12] sparked political revolutions,[13] and even launched a

---

Secretariat, Population Div. of the Dep't of Econ. & Soc. Affairs, *World Population Prospects: The 2008 Revision, Highlights* (2009), http://www.un.org/esa/population/publications/wpp2008/wpp2008_text_tables.pdf. As for the growth rate, in the United States alone, the number of Facebook users in the United States jumped from 42,089,200 on January 4, 2009 to 103,085,520 a year later. *See* Peter Corbett, *Facebook Demographics and Statistics Report 2010 – 145% Growth in 1 Year*, ISTRATEGYLABS (Jan. 4, 2010), http://www.istrategylabs.com/2010/01/facebook-demographics-and-statistics-report-2010-145-growth-in-1-year/. This represents a growth rate of 144.9%. *Id.*

7. *Press Room: Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 31, 2010).

8. *Id.*

9. For example, Facebook launched the marriage of two Kelly Hildebrandts when twenty-year-old Kelly Katrina Hildebrandt of Florida typed her name into Facebook to see if anybody shared it and met twenty-four-year-old Kelly Carl Hildebrandt of Texas. *See* Sam Jones, *Facebook Couple with Same Name to Marry*, GUARDIAN.CO.UK.COM (July 21, 2009, 14:10 BST), http://www.guardian.co.uk/world/2009/jul/21/same-name-couple-facebook-marry.

10. Unfortunately, as of this publication, only 94,530 had joined the group "Laura will name her baby Megatron if 100,000 people join this group!" *See Laura Will Name Her Baby Megatron if 100,000 People Join this Group!*, FACEBOOK, http://www.facebook.com/group.php?gid=7585598759&ref=search&sid=20905568.1841317061..1 (last visited Jan. 6, 2011).

11. Robbery charges against Rodney Bradford were dropped when he proved that, at the time of the robbery, he had changed his Facebook status to "Where's my pancakes" from his home. *See* Damiano Beltrami, *His Facebook Status Now? 'Charges Dropped'*, N.Y. TIMES, Nov. 12, 2009, at A27.

12. An Italian man who had been kidnapped by his father when he was

successful campaign to get eighty-eight-year-old national treasure Betty White invited to host *Saturday Night Live* for the first time in her half-century career.[14]

But the site's social benefits have also invited people to (over)share while lulling them into a false sense of privacy. People who joined Facebook during its infancy are quickly realizing that their online past is affecting their offline future. Facebook users are always one embarrassing photo away from their reputation being instantly ruined and ravaged before their entire network of family, friends, classmates, and colleagues. According to one study, 8 percent of companies with one thousand employees or more have terminated at least one employee for comments posted on a social networking site.[15]

Moreover, Facebook has proved to be a treasure trove of useful information for lawyers. The American Academy of Matrimonial Lawyers recently stated that a whopping 81 percent of its attorneys have used or faced evidence found on social networking sites like Facebook in divorce proceedings.[16]

In response to the rising tide of criticism regarding its privacy policies, Facebook now allows users to communicate with varying subjective levels of privacy expectations, just as in the non-digital world. In fact, the site arguably provides communication shields that some people lack in the real world; in densely-populated urban environments, people in a public

---

five years-old used Facebook to reunite with his Italian relatives after twenty-two years of living apart. *See Egypt: 'Italian child' appears in Cairo after 22 years*, ADNKRONOS INTERNATIONAL (Dec. 8, 2009), http://www.adnkronos.com/AKI/English/CultureAndMedia/?id=3.0.4083351836.

13. *See* Samantha M. Shapiro, *Revolution, Facebook-Style*, N.Y. TIMES MAG., Jan. 25, 2009, at MM34.

14. Lisa de Moraes, *Facebook Campaign for Betty White Pays Off: 'SNL' Posts Election-Season Numbers*, WASH. POST, May 11, 2010, at A06. As a joke, Ms. White stated in her opening monologue on *SNL* that she did not know what Facebook was, but after she found out, she concluded that "it seems like a huge waste of time[;]" the audience's laughter reflected a universal understanding of the truth underlying the joke. *Id.*

15. *See* Adam Ostrow, *Facebook Fired: 8% of US Companies have Sacked Social Media Miscreants*, MASHABLE.COM (Aug.10, 2009), http://mashable.com/2009/08/10/social-media-misuse (discussing survey by Internet security firm Proofpoint).

16. Leanne Italic, *Facebook is Divorce Lawyers' New Best Friend*, MSNBC.COM, June 28, 2010, http://www.msnbc.msn.com/id/37986320/.

space might struggle to converse without running the risk of being overheard.

Unlike most other social networking sites and Internet fora, Facebook provides users with many controls to determine who can view various categories of content. The potential readership begins with nobody and ends with everybody. Recluses like author Harper Lee[17] can use Facebook to communicate with one confidante, while exhibitionists like rocker Tommy Lee[18] can use it to broadcast hourly status updates to the world.

Yet, despite these privacy controls, every single one of Facebook's 120 million active users in the United States lack a reasonable expectation of privacy from unfettered government surveillance of their online activity. After all, in *Katz v. United States*, the Supreme Court stated that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[19] This Third Party Doctrine, if applied literally, leaves Facebook users with no expectation of privacy since any content on Facebook has been knowingly exposed to at least one third party (the Facebook staff) and, therefore, could be treated as if it were shared with the world.

Moreover, the Electronic Communications Privacy Act (ECPA), enacted in 1986, does not clearly apply to most of the communications on Facebook. Furthermore, under the statute, the government need not have probable cause or provide notice to compel disclosure of "private" information. In effect, only state laws and the court of public opinion prevent Facebook from giving the government carte blanche to fish through everything under the Facebook.com domain for incriminating

---

17. If Harper Lee does have a Facebook account, it is not open to the public. However, her fans created multiple Facebook pages devoted to her. *See, e.g.*, *Harper Lee*, FACEBOOK, http://www.facebook.com/pages/Harper-Lee/109379712415100?v=desc (last visited Nov. 1, 2010).

18. Tommy Lee, drummer for Mötley Crüe, has a Facebook page, which can be viewed by any member of the public, even without a Facebook account. *See Tommyleetv*, FACEBOOK, http://www.facebook.com/tommyleetv (last visited Nov. 1, 2010). While he uses his Facebook page to announce new projects and tours, he also uses it to share random thoughts, including the following message that he posted on September 5, 2010: "Fuck I'm Hungry!!!" *Id.*

19. 389 U.S. 347, 351 (1967).

evidence.

In this Article, I argue that a court does not faithfully apply *Katz* if it rules that *every* Facebook user lacks reasonable expectations of privacy with regard to personal information—e.g., every organizational affiliation, unshared photo, private message, unsent party invitation, and "poke"—even when the user opts for the strictest privacy controls, limits access to a sole recipient, and removes content immediately after uploading it. The majority in *Katz* could not have possibly intended that a friendless hermit who sporadically logs on to write a secret online diary enjoys the same privacy rights (or lack thereof) as an aspiring reality television star who shares videos of her every bacchanalian shenanigans with the world. Yet, in the world of Facebook, federal law offers the same minimal privacy protections to both the hermit and the narcissist.

This privacy void in many online communications leads to an absurd result: in an era when many communicate more online than in person, Facebook users in different towns might need to enter an archaic phone booth and close the door in order to expect privacy.

Given the growing awareness of privacy concerns presented by Facebook, one might conclude that its flaws will force users to migrate to a better site. Indeed, the rapid rate of technological change and the fickle nature of the digital era suggest that Facebook could soon go the way of MySpace and become the next "abandoned amusement park" of the Internet.[20] New social networking sites surface regularly, often employing new technologies and serving different purposes, but ultimately hoping to steal Facebook's traffic.[21]

Even though Facebook could do lots to improve its users'

---

20. Jon Swartz, *MySpace CEO Owen Van Natta Steps Down*, USA TODAY, Feb. 11, 2010, http://www.usatoday.com/tech/news/2010-02-11-myspaceceo_ST_N.htm.

21. For example, Flickr provides users with an opportunity to share and comment on photos. *About Flickr*, FLICKR, http://www.flickr.com/about/ (last visited Nov. 1, 2010). Yelp allows users to leave and read reviews of nearly everything. *About Us*, YELP, http://www.yelp.com/about (last visited Nov. 1, 2010). IJustMadeLove.com allows users to share where, when, and how they most recently engaged in intercourse. IJUSTMADELOVE, http://ijustmadelove.com/ (last visited Nov. 1, 2010).

consumer privacy rights, the issues of privacy from government surveillance originate with the government, not Facebook. Regardless of what social networking will look like in 2024 or whether our clones will have new ways to tap into new networks, one fact seems inevitable: in the digital world, social networkers will still store, access, and disseminate personal information through a third party. A digital community on the magnitude of Facebook will likely depend on some entity that functions as the server or hub for the content. While peer-to-peer networks suggest the possibility of direct communications without third party conduits, the very nature of the Internet makes it difficult to imagine a *social* network emerging in isolation without a person or entity hosting or facilitating the exchange. The resulting unreasonable expectation of privacy will thus follow those social networkers wherever they go unless there is congressional intervention or a judicial shift in how the Fourth Amendment is applied to online communications.

While this unique architectural feature has engendered the Facebook Effect, it also explains what I call the Facebook Defect: the failure of both the government and social networking sites to ensure that certain online communications receive the same probable cause standard set forth in the Fourth Amendment as they would offline. While the Facebook Effect has revolutionized the ways in which people communicate, the Facebook Defect has equally transformed the ability of governments around the globe to pry into the private lives of its citizens.

While modern wiretapping and other electronic recording devices might be more reminiscent of the law enforcement techniques depicted in *Nineteen Eighty-Four*, the government's ability to tap into social networking sites comes far closer to matching George Orwell's "Thought Police":

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate

> they could plug in your wire whenever they wanted to.[22]

What Orwell did not foresee, however, is that an omniscient "Big Brother" would result through government *inactivity*, as opposed to a totalitarian takeover. Indeed, criminal investigators now have access to an unsurpassed amount of private information thanks to the voluntary efforts of private citizens and the government's failure to ensure that privacy laws keep pace with changing technology.

Nonetheless, Facebook demonstrates Orwell's prognostications that one day the government would be able to tap into the thoughts and activities of its citizens. If that is not convincing enough, perhaps Orwell's prescience is best illustrated by this fact: Mark Zuckerberg, the CEO and co-founder of Facebook, was born in 1984.[23]

This Article seeks to analyze how the Fourth Amendment and federal statutes apply—and should apply—to evidence obtained on Facebook.

In the first Part, I will demonstrates how Facebook's architecture and policy changes provide enough nuanced and customized privacy controls to allow users to signal their intention to keep some data private.

In Part II, I will reveal the ways in which government agencies have investigated crimes by gathering evidence on Facebook.

In Part III, I will analyze how courts have interpreted the Fourth Amendment and the ECPA. Part IV will then apply these rules to Facebook and demonstrate how existing rules fail to protect information that most Facebook users assume is shielded from warrantless law enforcement searches.

Finally, in Part V, I make several proposals that faithfully apply *Katz* to Facebook and balance users' privacy concerns with the government's desire to collect evidence in criminal investigations. Specifically, I will offer a normative framework for applying the Fourth Amendment and the Third Party

---

22. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3-4 (1949).

23. *Mark Zuckerberg*, FACEBOOK, http://www.facebook.com/zuck (last visited Nov. 1, 2010).

Doctrine to social networking sites' (SNS) content and propose a statutory revision to the ECPA.

II. The Code of Facebook

"I'm trying to make the world a more open place."

- Facebook CEO and Co-Founder Mark Zuckerberg[24]

A. *Facebook's Architecture*

Facebook began as a closed social network that required registration with a university e-mail address from an Ivy League school. Slowly, Facebook was opened to all schools. Its initial exclusivity undoubtedly contributes to its publicity and popularity. By 2006, when the site was opened to the general public, "its clublike, ritualistic, highly regulated foundation was already in place."[25]

Today, Facebook asks its users to disclose a vast array of personal information, which explains why the site is such a treasure trove of evidence for government investigators. When joining, users are invited to post their:

- favorite music
- favorite books
- favorite movies
- favorite quotes
- address
- hometown
- phone numbers
- e-mail addresses
- clubs
- job
- job history
- educational history

---

24. *Id.*
25. Anderson & Wolff, *supra* note 2.

- birth dates
- sexual orientation
- interests
- daily schedules
- relation to friends
- pictures
- political affiliations

In addition to what users choose to divulge, Facebook "will receive information from [other third parties], including information about actions you take . . . even before you connect with the application or website."[26] Moreover, the site collects information about a user when "tagged" in a photo uploaded by another user. All of this information is "gathered regardless of your use of the web site."[27] Not only does Facebook collect this information, but it also disseminates this data to about five hundred thousand third-party application developers.[28]

But Facebook is far more than a corner of cyberspace where people poke friends and discuss common interests. More than 70 percent of Facebook users frequently visit the site to engage with other platforms—ranging from news-aggregating services to virtual livestock-raising games—some of which are only available through Facebook (and subservient to its platform).[29] Moreover, over a million websites and third-party applications allow users to interact through Facebook, even without actually visiting the Facebook site. Which is to say, if Facebook is a business parked on a specific corner of cyberspace, many active customers never visit, while its actual visitors are more likely looking for a million *other* businesses.[30]

---

26. *Facebook Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited Jan. 31, 2011).

27. *Id.*

28. Sarah Perez, *How to Delete Facebook Applications (and Why You Should)*, READWRITEWEB.COM, http://www.readwriteweb.com/archives/how_to_delete_facebook_applications_and_why_you_should.php (last visited Nov. 1, 2010).

29. *Id.*

30. This horrible sentence symbolizes the difficulty with analogizing cyberspace to real space. Please do not attempt this at home without adult supervision.

Today, Facebook's infrastructure hardly resembles the cyber-technology of only a decade earlier, when "using" an Internet-based service largely meant visiting a specific URL address on the World Wide Web. Today, users can communicate "through" Facebook without even visiting the Facebook.com domain. For starters, more than 150 million users access Facebook through a Facebook application on their mobile devices.[31]

Moreover, Facebook users increasingly use the site to access third-party platforms created by over a million developers from 180 different countries. These platforms have also been integrated into over a million websites outside of the Facebook.com domain.[32] Thus, Facebook allows a fan of the board game Scrabble, for example, to find a complete stranger to play against without actually visiting Facebook.[33]

B. *Facebook's Prior Privacy Policy*

Over its short existence, Facebook has repeatedly changed its privacy policies. Sometimes, the changes have been to the dismay of those concerned about privacy. At other times, the changes were in response to uproars about privacy.

But generally speaking, Facebook's policies have largely shifted from the default assumption of privacy to a default assumption of openness. Moreover, the policies have shifted from complete control over all information to partial control.[34]

For example, in 2005, Facebook's privacy policy stated:

> "No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy

---

31. *Press Room: Statistics*, *supra* note 7.

32. *Id.*

33. *See Scrabble on Facebook*, HASBRO.COM, http://www.hasbro.com/shop/details.cfm?guid=94365F4B-6D40-1014-8BF0-9EFBF894F9D4&product_id=23064&src=endeca (last visited Oct. 30, 2010).

34. Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline,* EFF DEEPLINKS BLOG (Apr. 28, 2010), http://www.eff.org/deeplinks/2010/04/facebook-timeline.

> settings."[35]

Two years later, however, the above language was removed and replaced with:

> Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.[36]

By November 2009, many more categories of information were included in the list of content that was available to everyone by default.[37]

While the reasons behind these changes were never fully explained, most observers recognize that the changes were a necessary first step toward achieving Facebook's long-term goal:

> Eventually, the company hopes that users will read articles, visit restaurants, and watch movies based on what their Facebook friends have recommended, not, say, based on a page that Google's algorithm sends them to. Zuckerberg imagines Facebook as, eventually, a layer underneath almost every electronic device. You'll turn on your TV, and you'll see that fourteen of your Facebook friends are watching "Entourage,"

---

35. *Id.* Note that Facebook was originally known as "Thefacebook" or thefacebook.com when introduced at Harvard University. Michael M. Grynbaum, *Mark E. Zuckerberg '06: The Whiz behind thefacebook.com*, THE HARVARD CRIMSON, June 10, 2004, http://www.thecrimson.com/article/2004/6/10/mark-e-zuckerberg-06-the-whiz/.

36. *Id.*

37. *Id.*

> and that your parents taped "60 Minutes" for you. You'll buy a brand-new phone, and you'll just enter your credentials. All your friends—and perhaps directions to all the places you and they have visited recently—will be right there.[38]

This vision of a customized recommendation system, dictated by trusted friends, requires that Facebook users be willing to disclose this information, of course. Given the low likelihood of users affirmatively going to their account settings and changing privacy policies, the alternative of requiring Facebook users to "opt in" to information-sharing would have jeopardized the company's long-term goal of global domination.

In addition to forcing users to affirmatively opt out of sharing information with others, Facebook has also made that process increasingly complex and unwieldy. In reviewing Facebook's current policy (discussed in the next section), the *New York Times* observed that "[t]o opt out of full disclosure of most information, it is necessary to click through more than 50 privacy buttons, which then require choosing among a total of more than 170 options."[39] Publications like the *Washington Post* have devoted entire pages to simply attempting to help Facebook users set privacy options.[40] Indeed, after Facebook announced its Places feature, it hilariously announced, "We've created a [four-minute long] video that explains our simple and powerful privacy settings."[41]

---

38. Vargas, *supra* note 5.

39. Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 12, 2010, http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=1.

40. *Help File: Facebook 'Places' Privacy Settings*, WASH. POST, Aug. 22, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/20/AR2010082006416.html.

41. FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=418175202130 (last visited Oct. 31, 2010). Keep in mind that this video is not about how to use the Places feature; it is merely an instructional video on the privacy options for the feature.

C. *Facebook's Current Privacy Policy*

Facebook's current policy, which became effective in December 2010, is now 5,954 words long.[42] Facebook's "Help Center" is available to assist users, but the word count for the privacy-related FAQ adds up to more than 45,000 words, which is almost twice as long as this Article, including the footnotes.[43]

While many aspects of Facebook's privacy policy form and affect users' expectations of privacy, the most relevant parts are discussed below:

1. "How We Share Information"

Section 6 of Facebook's current privacy policy, which was last revised on October 5, 2010, is titled "How We Share Information." The section begins with the following broad pronouncement:

> Facebook is about sharing information with others — friends and people in your communities — while providing you with privacy settings that you can use to restrict other users from accessing some of your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so.[44]

Users who read this preamble may justifiably conclude that, so long as they restrict access to specific individuals whom they trust, Facebook will not disclose any content to the government unless "legally required" to do so.

However, Facebook then lists the situations when it might share your information to other parties. Most pertinent to this

---

42. The *New York Times* noted that the previous policy was longer than the United States Constitution, which is 4,543 words without any of its amendments. Bilton, *supra* note 39.

43. *Id.*

44. *Facebook Privacy Policy*, *supra* note 26, § 6.

Article, the policy provides that:

> We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law.[45]

Thus, Facebook specifically announces that it "may" respond to mere government "requests," suggesting a standard far lower than reasonable suspicion or probable cause. The "required by law" part of the first sentence might be interpreted to mean that it will deny any "requests" unless it will face obstruction or contempt charges. However, as discussed in Part III and IV, what is "required by law" is a fuzzy standard.

The next sentence then states that it may also respond to requests for content outside of the United States:

> This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. [46]

This passage suggests that it will not be used to disclose the content of American users to other countries unless those users are "from" that jurisdiction. Thus, if a California citizen denies the Holocaust in her Facebook status and thereby violates the laws of Belgium, which explicitly criminalize Holocaust denials,[47] this policy suggests that Facebook would refuse to hand over any content.

---

45. *Id.*

46. *Id.*

47. Verfassungsgesetz vom 8. Mai 1945 über das Verbot der NSDAP (Verbotsgesetz 1947) in der Fassung der Verbotsgesetznovelle 1992, *available at* http://www.nachkriegsjustiz.at/service/gesetze/gs_vg_3_1992.php.

However, the final part of this paragraph from Facebook's privacy policy provides a broad catch-all disclaimer that seemingly dismantles the restrictions implied in the above passages:

> We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.[48]

Thus, under Facebook's policies, users are on notice that any evidence of "fraud," "illegal activity," or "imminent bodily harm" may be shared with any government entity, as well as "companies" and "lawyers."

2. "How You Can Change or Remove Information"

Another relevant part of Facebook's privacy policy is Section 7, which delineates what information Facebook archives and for how long. The policy states that "deactivating" an account will not result in the removal of any content, while "deleting" an account may result in permanent deletion:

> **Deactivating or deleting your account.** If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted. We save your profile information (connections, photos, etc.) in case you later decide to reactivate your account. Many users deactivate their accounts for temporary reasons and in doing so are asking us to maintain their information until they return to Facebook. You

48. *Facebook Privacy Policy*, *supra* note 26, § 6.

> will still have the ability to reactivate your account and restore your profile in its entirety. When you delete an account, it is permanently deleted from Facebook. You should only delete your account if you are certain you never want to reactivate it.[49]

This policy suggests that a Facebook user can confidently assume that his or her information is completely wiped out, thereby ensuring that no subpoena or warrant would allow such content to resurface. Later in this section, the policy makes clear "[r]emoved and deleted information may persist in backup copies for up to 90 days, but will not be available to others."[50]

Based on the above, a Facebook user might believe that after ninety days, any of his or her content will be permanently and irreversibly eliminated from existence. However, the policy makes clear that such an assumption would be incorrect.[51] The policy states that Facebook "may retain certain information to

---

49. *Id.* § 7
50. *Id.*
51. The policy states:

> **Limitations on removal.** Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users. However, your name will no longer be associated with that information on Facebook. (For example, if you post something to another user's profile and then you delete your account, that post may remain, but be attributed to an "Anonymous Facebook User.") Additionally, we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested. If you have given third party applications or websites access to your information, they may retain your information to the extent permitted under their terms of service or privacy policies. But they will no longer be able to access the information through our Platform after you disconnect from them.

Id.

prevent . . . other misconduct," suggesting that it might store some "deleted" content over ninety days old.[52] One interpretation of this is that Facebook only stores information on those whose content was requested via subpoena or warrant. Another interpretation is that Facebook is only guaranteeing its users recovery of their accounts for up to ninety days (perhaps to ensure that the request to delete was not a fraudulent request), but in reality, they will keep copies of everything for as long as they want.

3. "How We Protect Information"

In another part of the privacy policy, Facebook states that "[w]e do our best to keep your information secure" by keeping account information on a secured service behind a firewall.[53] However, it explicitly states that the only information that it encrypts "using socket layer technology (SSL)" is "sensitive information (such as credit card numbers and passwords)."[54]

This portion of the policy also makes clear that Facebook employees may use "automated and social measures" to "analyz[e] account behavior for fraudulent or otherwise anomalous behavior, may limit use of site features in response to possible signs of abuse, may remove inappropriate content or links to illegal content, and may suspend or disable accounts for violations of our Statement of Rights and Responsibilities."[55]

Finally, this section concludes with a general disclaimer warning users to never assume that their information will stay out of others' hands:

> **Risks inherent in sharing information.** Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of

52. *Id.*
53. *Id.* § 8.
54. *Id.*
55. *Id.*

> other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook.[56]

Thus, at this point, Facebook users are on notice that Facebook employees are monitoring their content and that its privacy-protecting measures are neither "perfect" nor "impenetrable."

4. "Other Terms"

Facebook's Privacy Policy concludes with the following passage, which has been roundly criticized by consumer privacy advocates:

> **Changes.** We may change this Privacy Policy pursuant to the procedures outlined in the Facebook Statement of Rights and Responsibilities. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account. If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. You can make sure that you receive notice directly by becoming a fan of the Facebook Site Governance Page.[57]

This policy effectively states that even if a user has a subjective and reasonable expectation of privacy with regard to various content, Facebook can unilaterally kill that expectation without affirmatively contacting her. A user would have to

---

56. *Id.*
57. *Id.* § 9.

check the Privacy Policy or the Facebook Site Governance Page on a daily basis to ensure that the policies have not changed. Even if one were to lose street credibility "by directly liking the Facebook Site Governance Page," she would not necessarily receive the notice of policy changes unless she logged in soon after the changes were made.[58]

This policy ended up being the source of much ire when Facebook recently announced that all users' names, profile photos, and the fact that they are Facebook users would be public information. Thus, a user who created a Facebook account in 2007 might have joined under the belief that only her selected "friends" would know that she was on Facebook. But today, all of her un-close friends and colleagues can find out that she has a Facebook account and grill her about why she has not "friended" them yet.

5. "How We Use Your Information"

Given Facebook's ability to unilaterally change its policy without your consent, one final policy is worth noting here:

> **Memorializing Accounts.** If we are notified that a user is deceased, we may memorialize the user's account. In such cases we restrict profile access to confirmed friends, and allow friends and family to write on the user's Wall in remembrance. We may close an account if we receive a formal request from the user's next of kin or other proper legal request to do so.[59]

In other words, if a Facebook user wants to be absolutely sure that her photos, list of friends, purchases, private messages, and Farmville scores will not be released to the general public for Google to permanently archive, she would be wise to heed the following advice: Don't die; keep yourself alive by checking the Facebook Site Governance Page every day.

---

58. *Id.*
59. *Id.* § 5.

D. *Facebook's Terms of Service*

Facebook's "Statement of Rights and Responsibilities," which was last revised on October 4, 2010, also provides that:

> 1. Privacy
>
> > Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.[60]

This statement does nothing to modify the privacy policies discussed above.

However, in the next section, Facebook reserves the right to distribute any content "covered by intellectual property rights," regardless of one's privacy settings. The policy states:

> 2. Sharing Your Content and Information
>
> > You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
> > For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete

60. *Facebook Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/policy.php#!/terms.php (last visited Oct. 30, 2010).

> your IP content or your account unless your content has been shared with others, and they have not deleted it.[61]

Later in the terms, Facebook defines the word "use":

> 17. Definitions
> . . .
> By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.[62]

In essence, Facebook owns most of your data.[63]

The policy seems designed to protect Facebook's right to reproduce and disseminate digital copies of a user's intellectual property without violating intellectual property statutes like the Copyright Act of 1976. For example, if the Facebook group "Students Against Backpacks with Wheels"[64] were to trademark a logo or create a music video promoting its message, the policy gives Facebook a legal right to display the logo and play the video on others' Facebook feeds.

Moreover, the "subject to your privacy and application settings" limitation suggests that Facebook does not have the license to distribute a user's intellectual property beyond the user's approved distribution list. Thus, if the Facebook group "Asian people with super White first-names, and super Asian

---

61. *Id.* § 2.

62. *Id.* § 17.

63. *See generally*, 18 U.S.C. §§ 101, 102, 106, 107, 117 (2005). Because copyrights do not rely upon registration like trademarks, a user's "status" may even be considered an original work created by copyright, assuming that the "tangible medium" rule of copyright law if fulfilled.

64. *Students against Backpacks with Wheels*, FACEBOOK, http://www.facebook.com/pages/GLOBAL/Students-Against-Backpacks-with-Wheels/229901724576?v=wall (last visited Oct. 30, 2010). Technically, this is a "page" and not a "group." However, according to Facebook's blog, "[P]ages were designed to be the official profiles for entities, such as celebrities, brands or businesses." Nick Pineda, *Facebook Tips: What's the Difference Between a Facebook Page and Group?*, THE FACEBOOK BLOG (Feb. 24, 2010, 4:40 PM), http://blog.facebook.com/blog.php?post=324706977130.

last-names :D"[65] were to create a baby-naming book intended for and only distributed to "fans," Facebook would presumably be restrained from disseminating the book beyond the approved list.

However, the above interpretations are based on limitations not clearly written into the contract. Indeed, one reasonable and textual interpretation of the policy is that, once a user has shared a photo with another person who does not "delete" the content, Facebook has an irrevocable license to distribute the photo to whomever it wants. Even if the user deletes the photo or closes her account, Facebook still maintains the license to distribute it since the "content has been shared with others, and they have not deleted it."[66]

On almost any other site, such ambiguities in the fine print of a policy on intellectual property would not trigger the barrage of angry privacy-related criticisms that Facebook has received. But in the context of Mark Zuckerberg's philosophy of openness[67] and Facebook's general movement toward liberating personal information, the concerns do not seem out of place. [68]

---

65. *Asian People with Super White First Names and Super Asian Last Names*, FACEBOOK, http://www.facebook.com/pages/Asian-people-with-super-White-first-names-and-super-Asian-last-names-D/111620102193432 (last visited Nov. 8, 2010). Unfortunately, because neither Westlaw nor Lexis allows a search for just ":D" due to their restrictions on searches for colons (of the punctuation variety), I am unable to confirm whether this is the first law review article to include an emoticon.

66. *Facebook Statement of Rights and Responsibilities*, *supra* note 60. Since most content on Facebook is not "received" in the same way that e-mail might be received in an inbox, the likelihood that a Facebook user "deletes" the content is low. The user would have to be motivated to somehow make an affirmative, conscious effort to ensure that she can never see the content again.

67. There is a certain irony in his championing openness since he is famously press-shy and weary of speaking to the public. *See, e.g.*, Vargas, *supra* note 5.

68. Of course, the openness championed by Zuckerberg has ultimately hurt Facebook's reputation, as details continue to emerge about Zuckerberg's cavalier views on user privacy. For example, in this verified instant message transcript, Facebook's CEO discussed the access he controlled to Harvard students' personal information:

> ZUCK: Yeah so if you ever need info about anyone at Harvard
> ZUCK: Just ask

E. *Other Social Networking Sites*

While Facebook has received more criticism over its privacy policies than any other SNS on the Internet, I would be remiss not to point out that other social networking sites have similar privacy rules with regard to sharing information with government authorities.

MySpace's privacy policy, for example, is even more amorphous and fuzzy than Facebook's policy with regard to when it may hand over your private information to the government:

> There may be instances when MySpace may access or disclose PII, Profile Information or non-PII without providing you a choice in order to: (i) protect or defend the legal rights or property of MySpace, our Affiliated Companies or their employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of Users of the MySpace Services or members of the public including acting in urgent circumstances; (iii) protect against fraud or for risk management purposes; or (iv) comply with the law or legal process.[69]

> ZUCK: I have over 4,000 emails, pictures, addresses, SNS
> [Redacted Friend's Name]: What!? How'd you manage that one?
> ZUCK: People just submitted it
> ZUCK: I don't know why
> ZUCK: They "trust me"
> ZUCK: Dumb fucks

Nicholas Carlson, *Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems*, BUSINESS INSIDER, May 13, 2010, http://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5. In an article that included interviews with Zuckerberg and other Facebook executives, the transcript was verified as true. *See* Vargas, *supra* note 5.

69. *Privacy Policy*, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=misc.privacy#ixzz10DCqHNzp (last visited Nov. 8, 2010).

Twitter is one of the largest social networks in the United States. Like Facebook, Twitter allows users to limit their "tweets" to specific users.[70] In their account settings, Twitter users can check a box that states "Only let people whom I approve follow my tweets." [71] But despite this privacy option, Twitter, like Facebook, makes clear in its privacy policy that users should not assume that any information is actually private:

> **Tweets, Following, Lists and other Public Information:** Our Services are primarily designed to help you share information with the world. Most of the information you provide to us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information. Our default is almost always to make the information you provide public but we generally give you settings to make the information more private if you want. Your public information is broadly and instantly disseminated. For example, your public Tweets are searchable by many search engines and are immediately delivered via SMS and our APIs to a wide range of users and services. You should be careful about all information that will be made public by Twitter, not just your Tweets.[72]

Elsewhere in Twitter's policy, the company makes clear that

---

70. *Twitter Privacy Policy,* TWITTER, http://twitter.com/privacy (last visited Nov. 8, 2010).

71. *See Twitter User Account Settings,* TWITTER, http://twitter.com/account/settings (last visited Jan. 7, 2011). If that box is not checked, the default is that the information is public. *See Twitter Privacy Policy*, *supra* note 70.

72. *Twitter Privacy Policy*, *supra* note 70.

any private information can be disclosed to the government upon a "legal request":

> **Law and Harm**: We may disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property.[73]

After reviewing the privacy policies of all top twenty five social networking sites,[74] I have concluded that they all refuse to limit the disclosure of personal information to responses to warrants or subpoenas. These other sites will disclose information to "comply with relevant laws,"[75] "unless required by law,"[76] or "when necessary to comply with a law."[77] In fact, a few SNS are more "cooperative" than Facebook, stating the intent to disclose any information that might possibly be illegal.[78]

---

73. *Id.*

74. Andy Kazeniac, *Social Networks: Facebook Takes Over Top Spot, Twitter Climbs*, COMPETEPULSE, http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/ (last visited Nov. 8, 2010).

75. *Privacy Policy*, STUMBLEUPON, http://www.stumbleupon.com/privacy/ (last visited Nov. 8, 2010).

76. *Delicious Privacy Policy,* YAHOO!, http://info.yahoo.com/privacy/us/delicious/ (last visited Nov. 8, 2010).

77. *About: Privacy Policy,* DIGG, http://about.digg.com/privacy (last visited Nov. 8, 2010).

78. Classmates.com, for example, states that it will disclose "as may be permitted or required by law, regulation, rule or court order; pursuant to requests from governmental, regulatory or administrative agencies or law enforcement authorities; or to prevent, investigate, identify persons or organizations potentially involved in, or take any action regarding suspected fraud, violations of our Terms of Service, or activity that appears to us to be illegal or may expose us to legal liability." *Privacy Policy,* CLASSMATES, http://www.classmates.com/cm/reg/privacy (last visited Nov. 8, 2010). Similarly, Meetup.com states that the user will "authorize us to disclose any information about you to law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability." *Meetup Privacy Policy Statement,* MEETUP, http://www.meetup.com/privacy/ (last visited Nov. 8, 2010).

III. How the Government Uses Facebook to Investigate

"If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place."

- Google CEO Eric Schmidt[79]

There is no doubt that the federal government is increasingly relying on social networking sites like Facebook to investigate crimes. After submitting a Freedom of Information Act request, the Electronic Frontier Foundation recently obtained a Justice Department memorandum that makes clear that the government does, indeed, use them.[80] According to the "UTILITY IN CRIMINAL CASES" portion of the memorandum, agents can use evidence from SNS to establish crime, provide location information, establish motives, prove and disprove alibis, and reveal communications.[81]

While no further specifics are provided, the broad categories suggest multiple ways in which Facebook serves as a valuable government investigative tool. For starters, agents can determine a suspect's friends and potentially yield informants or witnesses. They can comb through photos to look for stolen merchandise, weapons, or automobiles.

The site is also incredibly useful for prosecutors and police to identify and establish connections between individuals. For example, officers at the University of Illinois at Urbana-Champaign spotted two students urinating in public, but only managed to apprehend one of them, Adam Gartner.[82] When police asked about the other student's identity, Gartner falsely

---

79. Interview by Maria Bartiromo with Eric Schmidt, CEO, Google, (Dec. 3, 2009), *available at* http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people.

80. John Lynch & Jenny Ellickson, U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, *Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More*, (Mar. 2010), *available at* http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.

81. *Id.*

82. Kiyoshi Martinez, *Student Arrested after Police Facebook Him,* DAILY ILLINI, Aug. 1, 2006, http://www.dailyillini.com/news/2006/08/01/student-arrested-after-police-facebook-him.

claimed that he did not know him.[83] Gartner was eventually charged with obstruction of justice when the arresting officer obtained the other student's name from witnesses and established through Facebook that the two were friends.[84]

The ways in which government authorities have obtained information on Facebook vary, however. As will be discussed in Parts III and IV, the various ways in which government authorities have obtained information from Facebook pose different constitutional and privacy-related questions.

A. *Plain View*

Despite Facebook's privacy controls and the increasing awareness of privacy issues, much of the thirty billion pieces of content created each month remains viewable and searchable by the public.[85] There is no way to know why each of those pieces of content is public: a user may have intentionally sought to reveal it to the world, she may have been confused or mistaken about the privacy setting she chose, or she might have simply failed to make any active efforts to opt out of the public settings.

However, given the frequent changes to Facebook's privacy policy and the unwieldy process to opt out of sharing, which were discussed above, I suspect that consumer confusion and unawareness explain a substantial amount of the public content. To test this suspicion, I conducted a search for the exact phrase "new number is" on a website called YourOpenbook.org, which lets visitors search public Facebook updates using Facebook's own search service.[86] Openbook

---

83. *Id.*

84. *Id.*

85. In 2008, the Director of National Intelligence released a study that concluded that government-hired Internet investigators were able to find "noteworthy" results on social networking sites for over half of a study's 349 participants. Office of the Dir. of Nat'l Intelligence, *Considering Web Presence in Determining Eligibility to Access Classified Information: A Pilot Study*, (June 10, 2010), *available at* http://www.eff.org/files/20100514_odni_socialnetworking.pdf.

86. OPENBOOK, http://youropenbook.org/about.html (last visited Jan. 7, 2011). The site is entirely unaffiliated with Facebook; it merely operates as a search engine for publicly available Facebook information.

revealed over a hundred "hits" of Facebook users who revealed their new phone numbers.[87] While every announcement might have been intentionally broadcast to the world,[88] I suspect that most on the list would be surprised to learn that their new digits are public. For example, I doubt that Grayson Frederick, one of the many Facebook users whose public page was revealed in the search results, actually intended to tell the world that his "new number is 208 405 35[XX]" and that he has "unlimited txting so feel free to txt or call anytime."[89]

Regardless, I unearthed many articles covering criminal investigations conducted with the aid of Facebook; the majority of them involved evidence that was available to the public. Again, while this fact does not necessarily prove that the content was unknowingly shared to all, it is hard to assume that the thousands of Americans arrested because of evidence on Facebook were choosing to self-incriminate themselves.

For example, twenty-year-old Hadley Jons was ejected from a jury and found in contempt of court for posting on Facebook that "it's gonna be fun to tell the defendant they're guilty" before the defense even presented its case.[90] The defendant's lawyer's son discovered her post on Facebook during the trial by conducting searches for the jurors' names.[91] The judge ordered her to pay a $250 fine and write an essay on the Sixth Amendment.[92]

A different type of "plain view" took place when the

87. OPENBOOK, http://youropenbook.org/?q=%22new+number+is%22&gender=any (last visited Jan. 7, 2011).

88. Admittedly, the phone book in every city is a thick collection of people who consented to their names and phone numbers being freely disseminated.

89. Grayson Frederick, FACEBOOK (Sept. 26, 2010, 12:48 AM), http://www.facebook.com/profile.php?id=100000726944748&v=wall. I deleted the last two digits of his phone number in the unlikely event that there is an overlap between readers of the *Pace Law Review* and people likely to respond to Grayson Frederick's requests to "call anytime."

90. Martha Neil, *Oops, Juror Calls Defendant Guilty on Facebook, Before Verdict*, A.B.A J., Sept. 2, 2010, http://www.abajournal.com/news/article/oops._juror_calls_defendant_guilty_on_facebook_though_verdict_isnt_in.

91. *Id.*

92. *Id.*

Federal Bureau of Investigations (FBI) was hunting down Maxi Sopo, who was wanted in Seattle on bank fraud charges but managed to elude authorities.[93] When investigators learned that he had a private Facebook page with a public friend list, they learned that one of his friends happened to be a former employee of the Justice Department who was unaware of his alleged criminal escapades and contacted him.[94] With the help of the former employee, the FBI eventually captured and arrested Sopo—all without the need to resort to any warrants, subpoenas, or undercover reporting.[95]

While legal scholars may disagree about what types of content on social media sites are intended to fall within the "plain view" exception to the Fourth Amendment's search restrictions, there is one infamous arrest triggered by Facebook evidence that no self-respecting attorney would seek to exclude on Fourth Amendment grounds. On August 28, 2009, nineteen-year-old Jonathan G. Parker allegedly broke into a home in Fort Loudoun, Pennsylvania and stole two diamond rings worth more than $3,500.[96] He may not have ever been caught, but for the fact that the victim noticed on his computer monitor that somebody named Jonathan G. Parker had logged onto Facebook and failed to sign out of the account before leaving with the jewels.[97]

B. *Government Subpoenas, Warrants, and Requests*

Government entities seeking to subpoena electronic communication from Facebook or any other Internet service provider without the subscriber or member's permission must wade through a muddled maze of outdated laws. As discussed in Parts III and IV below, federal courts in both civil and

---

93. Sammy Rose Saltzman, *Partying Fugitive Maxi Sopo after Friending Fed on Facebook*, CBSNEWS.COM (Oct. 16, 2009, 9:44 AM), http://www.cbsnews.com/8301-504083_162-5383869-504083.html.

94. *Id.*

95. *Id.*

96. *See* Edward Marshall, *Burglar Leaves His Facebook Page on Victim's Computer*, JOURNAL-NEWS.NET (Sept. 16, 2009), http://www.journal-news.net/page/content.detail/id/525232.html.

97. *Id.*

criminal cases have inconsistently interpreted the constitutional and statutory protections on electronic data sought by a subpoena.[98]

However, as muddled as the law may be, Facebook has unilaterally simplified the requirements by requiring warrants for only private messages less than 181 days old. Through its spectacularly vague privacy policies, it has reserved the right to disclose all other content.[99]

In the Justice Department memorandum obtained by the EFF, the section titled "GETTING INFO FROM FACEBOOK" briefly discusses the "standard data productions" (or non-content) available: "Neoprint, Photoprint, User Contact Info, Group Contact Info, IP Logs."[100] But as for everything else, the memorandum cryptically states: "HOWEVER, Facebook has other data available. Often cooperative with emergency requests."[101]

Because the memorandum discusses data, policies, and experiences with multiple SNS, it makes clear that Facebook is far more "cooperative" than other sites. For example, "MySpace requires a search warrant for private messages/bulletins less than 181 days old" and "considers friend lists to be stored content."[102] The significance of this will be discussed in Part III.

C. *Fake Profiles*

The Justice Department memorandum obtained by the EFF also revealed that federal agents are creating fake identities on Facebook (among other SNS sites) to obtain

---

98. *Compare In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (holding that only unopened e-mail on an ISP server constituted "electronic storage"), *with* Theofel v. Farey-Jones, 359 F.3d 1066, 1076-77 (9th Cir. 2004) (holding that copies of opened e-mails on an ISP server constitutes electronic storage). These laws will be discussed more in detail *infra*.

99. *See Facebook Privacy Policy*, *supra* note 26. Because Facebook does not clearly offer any protections beyond those required by statute, it has implicitly reserved the right to disclose the contents of private messages without any warrant or subpoena.

100. Lynch & Ellickson, *supra* note 80, at 17.

101. *Id.*

102. *Id.* at 22.

evidence, search for witnesses, and track suspects.[103] Even though Facebook's policies ban Facebook users from providing false information or creating an account in another person's name, government agencies regularly create them in hopes that suspects (or suspects' friends) will approve the request and instantly allow them to access private information, map social networks, and begin the process of luring them into incriminating revelations.

In one section on working undercover on social networking sites, the document poses but does not answer the question: "[i]f agents violate terms of service, is that 'otherwise illegal activity'?"[104] No caselaw provides a clear answer. However, as discussed below, given the general legality of undercover operations in which officers violate crimes in order to prevent crimes, there seems to be no legal barrier to these fake profile tactics.

When asked about this technique, many police departments around the country have freely offered that they have "no reservations about going undercover on Facebook – taking on a fake identity and tricking a suspect into accepting a police department employee as a friend."[105] One officer defended the legality of the practice by stating that "[i]t's no different than putting on a pizza guy uniform and knocking on the door."[106]

Adam Bauer, a college student in Wisconsin, is one of many victims of this practice. Not long after he accepted an offer to become Facebook friends with "a good-looking girl" that he "randomly accepted this once for some reason," the La Crosse police invited him to the station, showed him photos from Facebook of him holding a beer, and then ticketed him for underage drinking.[107]

---

103. *Id.* at 32-33.

104. *Id.* at 32.

105. Julie Masis*, Is this Lawman your Facebook Friend?*, BOSTON GLOBE, Jan. 11, 2009, http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend?mode=PF.

106. *Id.*

107. KJ Lang, *Facebook Friend Turns into Big Brother*, LA CROSSE TRIBUNE, Nov. 19, 2009,

In an interview emphasizing Facebook's commitment to a "real name culture," Facebook spokesman Simon Axten stated that it "would not make an exception" with regard to the rule against assuming fake identities, even "for police officers working undercover."[108] Axten claims that the company "disable[s] the accounts of people operating under pseudonyms." However, the fact that this practice might violate Facebook's rules, and even the fact that violating Facebook's rules might itself constitute a crime,[109] still does not amount to a legal rule that prevents the police from engaging in this practice. This is discussed more in Part III-D below.

D. *Voluntary Disclosure from Facebook*

Facebook has openly acknowledged that it polices its site to protect children from sexual predators. As of January 2009, the company has removed more than 5,500 convicted sex offenders from its site.[110] Chris Kelly, Facebook's chief privacy officer, revealed some of its practices:

> We have devoted significant resources to developing innovative and complex systems to proactively monitor the site and its users, including those not on a sex offender registry, for suspicious activity (such as contacting minors or users of predominantly one gender).
>
> . . .
>
> If we find that someone on a sex offender registry is a likely match to a user on Facebook, we notify law enforcement and disable the account. In

---

http://lacrossetribune.com/news/local/article_0ff40f7a-d4d1-11de-afb3-001cc4c002e0.html.

108. Masis, *supra* note 105.

109. For example, a high school student in Georgia was recently arrested for criminal defamation for creating a Facebook account in the name of another student. Melissa Tune, *Teen Arrested for Fake Facebook Account in Teacher Firing Case*, WRDW.COM (Aug. 11, 2010, 4:09 PM), http://www.wrdw.com/crimeteam12/headlines/100284224.html.

110. Marlon A. Walker, *Facebook Gives Sex Offenders the Boot*, MSNBC.COM, Feb. 19, 2009, http://www.msnbc.msn.com/id/29289048/.

> some cases, law enforcement has asked us to leave the accounts active so that they may investigate the user further.[111]

Despite these proactive efforts, Facebook has been criticized for not doing enough to protect children,[112] especially after stories surfaced about how child abusers and rapists used Facebook to lure their underage victims.[113]

E. *Voluntary Disclosure from Third Parties*

Facebook users have often reported, forwarded, or provided law enforcement agents with access to evidence of crimes, especially when children or life-threatening emergencies are involved. For example, one Pennsylvania high school student's father was arrested by police when another student saw pictures of the party that he threw for students after a basketball game.[114] According to the affidavit, thirty-six-year-old Steven Russo hosted a basement party for underage high school students, provided them with rum and vodka, shared "sex stories about all the girls he has been with," and instructed the cheerleaders to use a stripper pole that he had installed.[115] The police obtained the photos after a student saw the photos on Facebook and shared them with the high school cheerleading coach, who handed them over to the police.[116]

---

111. Erick Schonfeld, *Thousands of MySpace Sex Offender Refugees Found on Facebook*, TECHCRUNCH (Feb.3, 2009), http://techcrunch.com/2009/02/03/thousands-of-myspace-sex-offender-refugees-found-on-facebook/.

112. *Id.* (suggesting that the ninety thousand registered sex offenders that MySpace had removed were making their way over to Facebook).

113. *See, e.g.*, Catharine Smith, *Serial Sex Offender Admits Using Facebook to Rape and Murder Teen*, HUFFINGTON POST (Mar. 8, 2010), http://www.huffingtonpost.com/2010/03/08/peter-chapman-admits-usin_n_489674.html.

114. *Dad's Teen "Stripper Pole" Party, Cops: Pennslyvania Man Threw Alcohol-Filled Basement Bash*, THE SMOKING GUN, Mar. 2, 2009, http://www.thesmokinggun.com/documents/crime/dads-teen-stripper-pole-party.

115. *Id.*

116. *Id.*

In other cases, authorities use Facebook to obtain leads, interview witnesses, or gain information on others. For example, police in Indiana, Pennsylvania were searching for two men who torched a couch after the Pittsburgh Steelers emerged victorious in Super Bowl XLIII. Despite the innate human need to burn furniture after a live sporting event, police nonetheless used publicly-available Facebook photos to find the suspects. Then, they contacted the owner of the page in which the photos were found; he identified them as Ryan Gould and Adam Alhabashi, who were arrested shortly thereafter.[117]

F. *Data-Mining Technologies*

Facebook's collection and aggregation of data has provided a vast amount of information to "responsible companies." There is no evidence that Facebook has provided this data to the United States government.

There was, however, a federal government agency that sought to collect the exact information that Facebook possesses. In 2002, it was discovered that the purpose of the Information Awareness Office (IAO), which is under the Defense Department's Defense Advanced Research Projects Agency (DARPA), was to gather as much information as possible about everyone in a centralized location for easy perusal by the government.[118] The IAO stated that its mission was to collect as much information as possible, including Internet searches, credit card activity, medical records, tax returns, airline purchases, educational transcripts, utility bills, car rentals, and driver's licenses.[119]

While there is no evidence of a direct relationship between Facebook and the IAO, they are, at most, only two degrees of separation apart. In 2005, Facebook received 12.7 million

117. *Facebook Pic Leads to Arrest in Super Bowl Celebration*, PITTSBURGHCHANNEL.COM (Feb. 6, 2009 11:17 A.M.), http://www.thepittsburghchannel.com/r/18656797/detail.html.

118. *See* John Markoff, *Pentagon Plans a Computer System that Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, http://www.nytimes.com/2002/11/09/politics/09COMP.html?pagewanted=1.

119. Jeffrey W. Seifert, Cong. Research Serv., RL31798, Data Mining and Homeland Security: An Overview 6 (2007).

dollars from the ACCEL venture capital firm, whose manager, James Breyer, sits on Facebook's board.[120] Breyer also founded a research and development firm known as BBN technologies, which hired Dr. Anita Jones,[121] who previously served as DARPA's Director of Research and Engineering[122] and oversaw the IAO's efforts to gather data on the nation's citizenry.

But more importantly, no direct relationship between Facebook and the IAO is needed to the extent that the government can still collect vast amounts of information from Facebook through any of the means listed above.

IV. Facebook Privacy under the Fourth Amendment

Criminal investigations by government officials are subject to the constraints of the Fourth Amendment of the United States Constitution, which provides:

> 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.[123]

Its "overriding function" is to "protect personal privacy and dignity against unwarranted intrusion by the State."[124]

The Fourth Amendment applies whenever a government

---

120. Erick Schonfeld, *Jim Breyer: Extra $500 Million Round for Facebook a "Total Fiction*," TECHCRUNCH, http://techcrunch.com/2007/11/02/jim-breyer-extra-500-million-round-for-facebook-a-total-fiction/.

121. *On the Move*, DEFENSE NEWS, Nov. 8, 2004, at 19, *available at* 2004 WLNR 23679109.

122. *Anita Jones*, UNIV. OF VA., http://www.cs.virginia.edu/people/faculty/faculty.php?member=jones (last visited Feb. 1, 2011).

123. U.S. CONST. amend. IV.

124. Schmberber v. California, 384 U.S. 757, 767 (1966).

official implements a search or seizure. Under the Fourth Amendment, a "search" includes searches of an individual, her pockets, private property, residence, office, hotel room, and luggage.

Prior to 1967, the Court interpreted the Fourth Amendment literally, such that only official searches of a person or his tangible effects were protected.[125] But since the Court's decision in *Katz v. United States*, the literal approach has been abandoned in favor of protecting "people, not places."[126] The Court held that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[127]

Katz implemented a two-step approach that looks to the reasonableness of a search or seizure.[128] Under this test, "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.'"[129]

For a search to be reasonable, government officials must usually obtain a warrant from a judge or magistrate by demonstrating probable cause to conduct a search.[130] Probable cause requires "reasonably trustworthy information" sufficient to "warrant a man of reasonable caution in the belief that an offense has been or is being committed" and that evidence will be found in the specific place to be searched.[131] A warrantless search is only reasonable if it falls into one of many exceptions to the rule, such as exigent circumstances,[132] "hot pursuit"

---

125. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

126. 389 U.S. 347, 352 (1967).

127. *Id.* (internal citation omitted)

128. *Id.* at 361 (Harlan, J., concurring).

129. *Id.*

130. U.S. CONST. amend. IV; *see also* Carroll v. United States, 267 U.S. 132, 156 (1925).

131. Brinegar v. United States, 338 U.S. 160,176 (1949) (citing Carroll v. United States, 267 U.S. 132, 156 (1925)).

132. Warden v. Hayden, 387 U.S. 294, 299 (1967); United States v. Santana, 427 U.S. 38, 43 (1976).

chases,[133] protective sweeps of a vehicle,[134] or searches of a person incident to a lawful arrest.[135]

A. *Plain View Exception*

With regard to SNS searches, the most relevant exception is that government officials do not need a warrant to observe something in "plain view." Under this rule, if a government official has a legal right to be in a specific location, she may obtain evidence that is in public or plain view.[136] Under the "open field" doctrine, this rule extends to warrantless administrative searches of outdoor property through the use of aerial photography.[137] This plain view exception engendered the three doctrines below, which further diminish the reach of the exclusionary rule.

B. *Voluntary Disclosure Doctrine*

The "voluntary disclosure doctrine," as announced by the Court in *Katz*, states that any information that is voluntarily conveyed to a third party does not receive Fourth Amendment protection.[138] Thus, the government does not engage in a Fourth Amendment "search" when using information a defendant disclosed to another individual, even when that conversation took place in private.[139] This doctrine would therefore apply to the overwhelming majority, if not all, content on Facebook since it is information that a Facebook user voluntarily agrees to have held in third party storage.

---

133. *Hayden*, 387 U.S. at 310 (Fortas, J., concurring).
134. United States v. Ross, 456 U.S. 798, 809 (1982).
135. United States v. Robinson, 414 U.S. 218, 234 (1973).
136. See v. City of Seattle, 387 U.S. 541, 545 (1967).
137. Dow Chem. Co. v. United States, 476 U.S. 227, 235 (1986).
138. *Katz*, 389 U.S. at 351.
139. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 574 (2007).

C. *Private Search and Seizure Doctrine*

The principles behind the voluntary disclosure doctrine have been further stretched to mostly forbid the exclusionary rule from extending to "private" or nonpolice searches. In *Burdeau v. McDowell*, the Court held that the history of the Fourth Amendment was intended to restrain "the activities of sovereign authority" and not intended to limit anyone else.[140] Indeed, even if a private person such as a "mall cop" or private detective has the role of investigating criminal conduct, then the Court would likely admit the evidence.[141] Thus, there is usually no reasonable expectation of privacy to information that someone voluntarily discloses to a third party who independently chooses to forward the material to the police. However, if the government orders, requests, helps plan, or tacitly approves a private person's search, the Court has applied the exclusionary rule.[142]

D. *Misplaced Trust Doctrine*

Another important spinoff of the plain view rule is the misplaced trust doctrine, which may apply when a Facebook user voluntarily discloses information to someone who turns out to be an undercover officer.[143] Under this doctrine, a person who mistakenly places her trust in someone who turns out to be an informant or government agent does not maintain any privacy rights under the Fourth Amendment.[144] The Court has repeatedly refused to adopt the rule that "the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not

140. 256 U.S. 465, 475 (1921).

141. *See, e.g.*, United States v. Francoeur, 547 F.2d 891 (5th Cir. 1977) (holding that search by security personnel of privately-operated amusement park did not amount to violation of Fourth Amendment rights).

142. *See* Walter v. United States, 747 U.S. 649 (1980).

143. *See* Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963).

144. *See, e.g.*, Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493 (2007).

reveal it."[145]

Thus, the government has the authority to use undercover operatives to prevent crime.[146] More specifically, the Ninth Circuit has held that government officials must be allowed to take on reasonable false identities in order to be more convincing in their undercover operations.[147]

Accordingly, undercover agents can use deception to procure consent to a search. In *Hoffa v. United States*, for example, the Court noted the possibility that someone will be observed by undercover officers is "the kind of risk we necessarily assume" and "inherent in the conditions of human society."[148] While some questioned *Hoffa*'s validity after *Katz*, the Court in *United States v. White* reaffirmed the rule that a person does not have any "justifiable expectation of privacy" when making incriminating statements to an informer.[149]

No federal statute or court has yet had occasion to draw any boundaries or rules regulating undercover policing on the Internet. Thus, suppose that Semion Mogilevich, who is on the FBI's list of Top Ten Most Wanted Fugitives, has a Facebook page.[150] Would a government agent be forbidden from creating a Facebook account in Semion's mother's name, uploading an actual photo of her, and naively hoping that he might divulge his whereabouts? While virtually every government agent to whom I asked this question concluded that this would be "going

---

145. Hoffa v. United States, 385 U.S. 293, 302 (1966).

146. Jacobson v. United States, 503 U.S. 540, 548 (1992).

147. *See* United States v. McQuin, 612 F.2d 1193, 1195 (9th Cir. 1980).

148. *Hoffa*, 385 U.S. at 303 (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).

149. 401 U.S. 745 (1971). Technically, only a four-person plurality held that a person does not have any "justifiable expectation of privacy" when making incriminating statements to an informer. However, Justice Black concurred because he believed the Fourth Amendment was inapplicable to conversations.

150. *FBI - Semion Mogilevich*, FBI, http://www.fbi.gov/wanted/topten/fugitives/mogilevich_s.htm (last visited Nov. 8, 2010). There is a Semion Mogilevich who has a Facebook page. *Semion Mogilevich*, FACEBOOK, http://www.facebook.com/people/Semion-Mogilevich/100000602506384 (last visited Jan. 31, 2011). Unfortunately, I do not know whether the user is actually named Semion Mogilevich or whether he is the person wanted by the FBI. Unfortunately, my passion for scholarly research stops at sending friendship requests to wanted criminals.

too far," neither the agents nor I have found any federal precedent restricting such a deceptive practice.

Thus, only state law or a congressional statute can protect private conversations from being surreptitiously documented. For example, the Massachusetts Supreme Court interpreted Article 14 of the state's Declaration of Rights to mean that its citizens can reasonably expect that their private conversations held in private homes are not being electronically transmitted or recorded by undercover government agents.[151]

E. *Application of the Fourth Amendment to New Technologies*

But courts have struggled to apply all these rules—which often assume a search in "real space" for a tangible document or an audible conversation—to the digital world. Because very few courts have addressed the application of the Fourth Amendment to content searches on third party servers, this Part provides a brief summary of the caselaw that has been used, by analogy, to Internet searches.

1. Postal Service Searches

Since the late 1800s, the Supreme Court has applied the Fourth Amendment to various forms of communication between citizens in different homes. In *Ex Parte Jackson*, the Court applied the Fourth Amendment's warrant requirement to sealed letters sent through the Postal Service.[152] The Court held that:

> Letters, and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles . . . . Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation,

151. Commonwealth v. Blood, 507 N.E.2d 1029, 1033 (Mass. 1987).
152. 96 U.S. 727, 733 (1877).

> particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.[153]

The essence of Justice Field's mail privacy rule from *Ex Parte Jackson* remained in place for over a century. A congressional statute codified the rule:

> No letter of such a class of domestic origin shall be opened except under authority of a search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the letter can be delivered, or pursuant to the authorization of the addressee.[154]

However, President George W. Bush amended the rule to allow searches "in exigent circumstances, such as to protect human life and safety against hazardous materials, and the need for physical searches specifically authorized by law for foreign intelligence collection."[155] Also, this rule does not apply when sealed mail originates beyond the borders of the United States[156] or is sent through Fourth Class mail.[157]

2. Telephone Searches and Electronic Surveillance Unrelated to Computers

When first faced with the issue in 1928, the Court held that wiretapping telephone conversations did not trigger the Fourth Amendment.[158] In *Olmstead v. United States*, Chief

153. *Id.*

154. 39 U.S.C. § 3623(d) (repealed 2009).

155. Press Release, George W. Bush, President's Statement on H.R. 6407, the "Postal Accountability and Enhancement Act," Dec. 20, 2006, *available at* 2006 WL 3737548.

156. *See* United States v. Various Articles of Obscene Merchandise, Schedule No. 1213, 395 F. Supp. 791 (S.D.N.Y. 1975), *aff'd*, 538 F.2d 317 (1976).

157. *See* United States v. Riley, 554 F.2d 1282, 1283 (5th Cir. 1977).

158. Olmstead v. United States, 277 U.S. 438, 464 (1928).

Justice Taft's majority opinion compared a telephone call with an audible conversation between two individuals in an open public space.[159] In a famous dissent, Justice Brandeis stated that telephone users enter a virtual private space, even if the wires being tapped are in public space.[160]

Today, the law on telephonic wiretapping searches largely resembles the law on mail searches, in that private phone calls are treated like private packages. In *Katz v. United States*, the Court reversed the rule from *Olmstead* and analogized the act of entering a closed public phone booth to the act of entering a private building.[161] The Court held that the government's electronic surveillance and recording of Katz's conversation in the phone booth violated his "reasonable expectation of privacy," and thus, also infringed upon his Fourth Amendment rights.[162] Under this rule, a person must exhibit both an "actual (subjective) expectation of privacy" and "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[163]

But just as some mail is unprotected, there are also limitations to telephonic privacy. In *Smith v. Maryland*, the Court held that the phone number a person dials is not protected since that information must be revealed to someone at the phone company in order for the call to be made.[164] The Court reasoned that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[165] The opinion noted that the numbers obtained by the pen register "do not acquire the 'contents' of communication," thereby distinguishing the phone numbers from the conversations recorded in *Katz*.[166]

In 1979, the Supreme Court further expanded the use of

159. *Id.*

160. *Id.* at 471 (Brandeis, J., concurring).

161. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

162. *Id.* at 362. Although the "reasonable expectation of privacy" rule stems from Justice Harlan's concurrence, virtually every court recognizes that the genesis of the doctrine originates with *Katz*.

163. *Id.* at 361.

164. Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

165. *Id.* at 743-44.

166. *Id.* at 747-48 n.1 (Stewart, J., dissenting).

electronic surveillance orders in *Dahlia v. United States*.[167] In that case, the Court held that the Fourth Amendment permits the government to secretly enter private property to install electronic surveillance devices with a warrant or an order under electronic surveillance law.[168] *Dahlia* helped pave the way for a dramatic uptick in the number of approved electronic surveillance orders: whereas only 174 orders were approved in 1968, there were 461 federal orders and 1,378 state orders approved in 2006.[169]

3. Bank Record Searches

The Supreme Court's 1976 decision in *United States v. Miller* plays a major role in Internet-related searches today, despite the fact that the case involved no question of emerging technology.[170] In *Miller*, the Court was faced with the question of whether a person has privacy rights in the financial records that he shares with a private bank. The Court distinguished "private papers" from "the business records of the bank," concluding that bank records are unprotected since a defendant could "assert neither ownership nor possession" over those papers.[171] The Court reasoned that *Miller* had no reasonable expectation of privacy in those records because he voluntarily disclosed them to a third party, his bank.[172] In other words, he "assumed the risk" that the bank may reveal his information to the government.[173]

---

167. United States v. Miller, 441 U.S. 238 (1979).

168. *Id.*

169. *See* Electronic Privacy Information Center, *Title III Electronic Surveillance 1968-1999*, EPIC, http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html (last visited Nov. 15, 2010). 92 percent of the wiretaps in 2006 involved mobile devices. James C. Duff, Director, Administrative Office of the U.S. Courts, *Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* (Apr. 2007), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2006/2006WT.pdf.

170. 425 U.S. 435 (1976).

171. *Id.* at 440.

172. *Id.* at 443.

173. *Id.*

This "assumption of risk" reasoning from *United States v. Miller* paved the way for *Smith v. Maryland* and the Third Party Doctrine. Together, *Miller* and *Smith* establish that Internet customers and users do not have reasonable expectations of privacy in their transactional records or subscriber information. This doctrine will play a major role in Internet-related searches, discussed infra.

4. Computer Hardware Searches

In the United States, "[i]ndividuals generally possess a reasonable expectation of privacy in their home computers."[174] Thus, generally speaking, the government can only seize and search a person's computer with a warrant.[175] Some cases have upheld broad searches of a person's entire computer system,[176] while others have limited the scope to those files sought by the warrant.[177] Computer searches have also been limited when a computer is shared by different users and certain files are protected by different passwords.[178] However, when a person makes his home computer available to his family members and his spouse ends up accessing personal information on the hard drive and using it against him in court, a court may not necessarily protect such accessible data.[179]

---

174. *See* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

175. *See* United States v. Lacy, 119 F.3d 742 (9th Cir. 1997). Presumably, some of the warrantless search exceptions such as plain view and consent searches can be applied to computer searches.

176. *Id.* at 746; *see also* United States v. Campos, 221 F.3d 1143 (10th Cir. 2000).

177. *See* United States v. Carey, 173 F.3d 1268 (10th Cir. 1999) (excluding the discovery of pornographic files when the warrant was limited to searching for records about illegal drug distribution). For an excellent article on the difficulty of applying traditional Fourth Amendment doctrine to computer searches, see Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 556 (2005).

178. *See* Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (concluding that one person's consent to search did not extend to a search of another user's files on the same computer when that person did not know the other's password).

179. White v. White, 781 A.2d 85 (N.J. Super Ct. Ch. Div. 2001) (holding there was no objective, reasonable expectation of privacy in e-mails stored on family computer's hard drive)

Over the last five years, government searches of a home computer have also raised new questions because of the possibility that a person's files, stored on a computer at home, can be searched through peer-to-peer networks. Thus far, the Eighth, Ninth, and Tenth Circuits—the only circuits that have confronted this issue—have all ruled that defendants lack a reasonable expectation of privacy in files that are freely shared with others.[180]

For example, in *United States v. Stults*, the defendant had child pornography files on his home computer but unknowingly shared them through his peer-to-peer file-sharing software.[181] As a result, the federal government was able to search and duplicate the files.[182] Even if defendant was unaware that others could access those files, the Eighth Circuit nonetheless held that he lacked a reasonable expectation of privacy in any shared files.[183]

These cases were easy to decide, in my view, because the incriminating files were in plain view. From the perspective of an outsider using a file-sharing program, the defendants in those cases did nothing to password-protect, conceal, or block complete strangers from accessing files. Although some of the defendants claimed to be unaware that incriminating content was being shared, that explanation is no different than saying, "I was unaware that the curtains in my house were open and that others could see my crystal meth lab." People who share files on a peer-to-peer network are aware that complete strangers can duplicate their files; as such, they cannot argue they expected to somehow distinguish between the police and private individuals.

---

180. United States v. Borowy, 2010 WL 537501, at *3 (9th Cir. Feb. 17, 2010); United States v. Stults, 575 F.3d 834, 843 (8th Cir. 2009), *cert. denied*, 130 S. Ct. 1309 (2010); United States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007) (holding that a city employee did not have a reasonable expectation of privacy in his personal computer that he brought to work and hooked up to the city's network for file sharing, kept continuously on, and failed to password protect).

181. *Stults*, 575 F.3d at 834.

182. *Id.*

183. *Id.*

5. Searches of Digital Content Stored on Third Party Servers

This category squarely addresses the technological search discussed by this Article: government searches of information that users store, send, or receive through the Internet. Unlike the previous category, the information obtained is not literally found on a person's home computer, but rather, on a server, outside the home, hosted by a third party.

When an electronic communication stored on another server is readily viewable to the public, courts have had no difficulty applying the "plain view" rule to such content. For example, courts have refused to find a reasonable expectation of privacy with regard to content on websites open to the public.[184] In *United States v. Gines-Perez*, a district court refused to exclude a picture of a store's employees that a government agent downloaded from a store's website.[185]

Another relatively settled rule in this area is that courts have extended the *Miller* and *Smith* Third Party Doctrine rules to network accounts and other non-content information obtained from Internet service providers (ISP). As the Tenth Circuit observed, "[e]very federal court to address this issue has held that subscriber information provided to an Internet provider is not protected by the Fourth Amendment's privacy expectation."[186] For example, in *Guest v. Leis*, the Sixth Circuit

184. *See* Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4, 27 (D. Mass. 2002), *rev'd*, 329 F.3d 9 (1st Cir. 2003); U.S. v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002); J.S. *ex rel.* H.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412 (Pa. Commw. Ct. 2000), *aff'd*, 569 Pa. 638 (2002) (holding that a minor did not have a reasonable expectation of privacy as to content on his website).

185. *Gines-Perez*, 214 F. Supp. 2d at 225.

186. United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); *see also* United States v. Forrester, 495 F.3d 1041 (9th Cir. 2007), *amended on other grounds by* 512 F.3d 500 (9th Cir. 2008) (holding that e-mail and Internet users have no reasonable expectation of privacy in source or destination addresses of e-mail or the IP addresses of websites visited); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (refusing to protect network account holders' subscriber information from communication service provider); United States v. Hambrick, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion); United States v. Kennedy, 81 F. Supp. 23 1103 (D. Kan. 2000); Hause v. Com., 83 S.W.3d 1 (Ky. Ct. App. 2001); United States v. Cox, 190 F. Supp. 2d

held that the Fourth Amendment did not protect ISP customers' subscriber information because they were voluntarily communicated with "systems operators."[187] These conclusions are largely consistent with the telephone and mail rules, to the extent that one can analogize a customer's subscriber information with the phone number provided to a telephone operator or the address in plain view of the postal service; none of these examples involve government searches of "conversations" or other content-rich information.

In essence, if a person does nothing to manifest an intention to keep electronic content private, then there is no reasonable expectation of privacy. Courts have reached different conclusions, however, when a person does take some active steps to keep content private.

While there is hardly enough caselaw to identify a general trend, most courts facing this question refused to protect "non-content," applying similar principles from caselaw involving postal mail and telephone calls.

For example, in *United States v. Forrester*, the Ninth Circuit held that a pen register that monitored a criminal defendant's Internet usage did not constitute a search.[188] When PacBell installed a "mirror port," the government was able to learn "the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account."[189] Despite the advanced technology involved, the court held that the surveillance was "conceptually indistinguishable from government surveillance of physical mail" and telephone calls.[190]

In contrast, a New Jersey state court, interpreting the state constitution, held that a defendant had a reasonable expectation of privacy in her ISP account information because

---

330 (N.D.N.Y. 2002).

187. *Guest*, 255 F.3d at 336; *see also Kennedy*, 81 F. Supp. 2d at 1110; *Hambrick*, 55 F. Supp. 2d at 508 (holding that ISP records were not protected since the defendant knowingly revealed his name, address, credit card number, and telephone number to Mindspring and its employees).

188. United States v. Forrester, 495 F.3d 1041, 1048 (9th Cir. 2007).

189. *Id.* at 1044.

190. *Forrester*, 495 F.3d at 1041.

her use of an anonymous ISP "screen name" manifested her intention to keep her identity anonymous.[191] Similarly, the First Circuit affirmed a Rhode Island district court decision that held that the government's right to access a public library computer network did not extend to the right to access a city official's private Yahoo! e-mail user's account that was accessed on that network.[192]

However, even where courts have found a reasonable expectation of privacy in digital content stored on third party servers, the government has still been able to compel the production of content by way of a subpoena.[193] The Supreme Court has previously held that the Fourth Amendment is not violated by a subpoena that is "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[194] Moreover, the Fourth Amendment does not require that the targets of an investigation in third-party subpoena cases be notified.[195]

The fact that the third party may not "own" the requested content is irrelevant; so long as the entity has "access" or "control" to the content, the government may compel disclosure.[196] Because most network service providers include terms of service that state that the providers have authority to access and disclose a subscriber's content, courts have had no difficulty concluding that the providers had "access" or "control" to the content.[197]

But unlike the rules on inspecting "content" in mail and

191. State v. Reid, 914 A.2d 310, 317 (N.J. Super. Ct. App. Div. 2007).

192. Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006). The court did not conclude, however, that all Yahoo! e-mail users have a reasonable expectation of privacy in their e-mails.

193. *See, e.g.*, United States v. Palmer, 536 F.2d 1278, 1281-82 (9th Cir. 1976).

194. Donovan v. Lone Steer, Inc., 464 U.S. 408, 414-15 (1984) (quoting *See*, 387 U.S. at 544).

195. *See* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743, 749-51 (1984).

196. *See* United States v. Matlock, 415 U.S. 164, 171 n.7 (1974); *see also* United States v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (allowing disclosure of a defendant's mail that was in the possession of a third party's mail service).

197. *See* Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (en banc).

telephone calls, most courts have not extended similar Fourth Amendment privacy rights to people who create, send, or receive content on third party servers. While the law in this area is still in its infancy, the Third Party Doctrine has played a major role when courts explain why a person does not have a reasonable expectation of privacy in content stored on the Internet.[198]

First, in the employment context, the Supreme Court recently held that employees that communicate through employer-provided network servers or on employer-supplied technologies do not have a reasonable expectation of privacy in their communications.[199] The Court's ruling reflects the fairly large consensus among the lower courts.[200] Even when an employee has taken measures to shield messages sent over his work e-mail by placing them in a "personal folder," the fact that these messages travel through the employer's network—subjecting them to third party access—strip them of any Fourth Amendment protections.[201]

Courts have similarly refused to protect chat room communications, bulletin boards, and e-mails forwarded to "lists" created from all chat room members. In *Guest v. Leis*, the Sixth Circuit held that a disclaimer on a private bulletin board service defeated any expectation of privacy in postings.[202] In *United States v. Charbonneau*, a district court held that, while a person can reasonably expect that an e-mail, like a letter, will not be intercepted prior to reaching the recipient without a warrant, once the recipient receives that e-mail, any privacy expectation is greatly diminished.[203] The court noted that the sender cannot control the fate of a message once it is received, whether by a recipient that intends to share the

198. I am using the phrase "on the Internet" as a short-hand way of saying "on servers hosted by Internet service providers and other third parties that hold content belonging to an individual."

199. *See* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

200. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *1 (Tex. Ct. App. May 28, 1999).

201. *McLaren*, 1999 WL 339015 at *4.

202. *Guest*, 255 F.3d at 333.

203. United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997).

content, or by an undercover agent.[204]

Thus, courts have fixated on this architectural difference between telephone conversations (during which people do not expect to be taped) and Internet communications (where messages are "recorded" and can be easily forwarded).[205] Unlike a telephone conversation, during which the persons communicating would have no reason to believe that the content of their communications were being taped or recorded, users of the Internet are aware that their communications and messages are being conducted in a recorded format.[206]

Indeed, thus far, only two military courts have found a reasonable expectation of privacy, under the Fourth Amendment, in stored e-mail messages.[207] No other courts reached a similar result.

The reason that the caselaw is so thin is that most courts have been able to avoid these questions because of federal statutes that extend privacy rights beyond those guaranteed by the Fourth Amendment.

F. *Application to Facebook*

1. Information in Plain View

Facebook users who make their profile "public" have no reasonable expectation of privacy since any evidence obtained from the site is clearly in "plain view." The Fourth Amendment's warrant requirement will not apply when a government investigator can freely view a website without any

---

204. *Id.* at 1184-85.

205. Com v. Proetto, 771 A.2d 823 (Pa. 2001), *appeal granted in part*, 790 A.2d 988 (Pa. 2002) *and order aff'd*, 837 A.2d 1163 (2003) (holding there was no reasonable expectation of privacy in e-mail messages sent by man to a fifteen-year-old girl where e-mail communications, including two photographs, were sent to the girl after the two chatted in an online chat room).

206. *Id.*

207. *See* United States v. Long, 64 M.J. 57, 66-67 (C.A.A.F. 2006); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (concluding that the accused had a reasonable expectation of privacy in e-mail files stored by AOL).

special passwords or encryption tools.

Granted, a person's Facebook page may not be in plain view in the same way as, say, marijuana plants in a person's backyard.[208] Unlike the crops, it is unlikely that an officer might see a person's Facebook page through a routine patrol. However, the website is something the police can see with the naked eye without resorting to mechanical devices "not in general public use."[209]

Facebook users who mask or alter their true identities—by using nom de plumes or fake profile photos, for example—still lack a reasonable expectation of privacy if the public can nonetheless view their content. The intent to mask identity is not the same as the intent to keep the incriminating evidence private. Any information obtained would be in "plain view" and could, among other things, provide the probable cause necessary to obtain a warrant to learn the user's true identity.

Indeed, a handful of friends and former students, when transitioning into a professional career or looking for jobs, have invited me, again, to their second Facebook account.[210] Most claim that the privacy policies are not effective enough to ensure that their new "professional" self will clearly exclude incriminating photos and the friends likely to post inappropriate content. Indeed, Norton's 2010 Cybercrime report revealed that one-third of seven thousand adults in fourteen countries have "used a fake online identity."[211] Meanwhile, no caselaw suggests that evidence in plain view of a police officer should be excluded because the officer did not

---

208. *See* California v. Ciraolo, 476 U.S. 207 (1986) (holding that the marijuana, which was viewable by any person who flew above the airspace, fell within the plain view doctrine).

209. Kyllo v. United States, 533 U.S. 27 (2001) (holding that the use of a thermal imager to detect infrared radiation inside a person's home was a search).

210. This does clearly violate Facebook's policies. Facebook insists that each individual have one account and use the privacy options to differentiate between, for example, employees, friends, and family.

211. Marian Merritt, *Norton's Cybercrime Report: The Human Impact Reveals Global Cybercrime Epidemic and Our Hidden Hypocrisy*, NORTON COMMUNITY (Sept. 8, 2010), http://community.norton.com/t5/Ask-Marian/Norton-s-Cybercrime-Report-The-Human-Impact-Reveals-Global/ba-p/282432.

know the true identity of the perpetrator.

2. Information Forwarded to the Government by a Facebook "Friend"

Any information that a private Facebook user's "friend" willingly gives to a government official will not be excluded since private searches do not trigger the Fourth Amendment. For example, suppose a mother sees on her teenager daughter's computer monitor that some of her Facebook friends are running a counterfeit stamp operation and reveals this information to the police. Even if the counterfeiters set their profiles to be viewable only by a limited set of friends, and even if they never imagined that someone's mother would see the page, no government search has taken place.

However, it does not follow that a Facebook user lacks reasonable expectation of privacy simply because another "private" person *could* pass on the content to a police officer. After all, the person to whom Katz was speaking could have repeated the content of the conversation to the police.

One gray area involves situations where private individuals provide police with evidence or information of illegal activity on Facebook, but then the police ask her cooperation to broaden the search. Suppose Bernardo, who is Facebook friends with Tony, tells Officer Krupke that he saw photos on Facebook of Tony trespassing on private property. Officer Krupke then asks Bernardo to come into the station and show him the photos. But after Bernardo logs into his Facebook account and hands Officer Krupke his laptop, the officer begins to snoop for additional evidence or additional crimes.

Such a search might conflict with existing caselaw regarding searches in physical spaces where the police go beyond the allowed physical scope of the search. For example, in *Thompson v. Louisiana*, the Supreme Court held that a daughter's summoning police to her mother's home to render medical assistance did not constitute an open-ended invitation for the police to conduct a general search for evidence of

homicide.[212]

Such a search may also run afoul of cases restricting third persons, in certain contexts, to consent to searches of jointly owned property. As a general rule, a third party who shares common authority over property can consent to a search and waive the Fourth Amendment rights of the other.[213] However, the consent may evaporate when the third party is no longer present.[214] For example, the First Circuit suppressed an audio recording after an undercover agent rented a hotel room for a defendant and planted recording devices.[215] Even though the government claimed that it did not record when the consenting undercover agent was absent, the court held that "when one's confidante leaves his premises, he is left with an expectation of privacy in his surroundings which is not only actual but justifiable."[216] Similarly, the district court in *United States v. Shabazz* held that a defendant's companion's consent to wire a rented hotel room for audio and video recording, even when the companion was not in the room, was "so massive and unregulated as to require the suppression of its product."[217]

No court has had occasion to apply these principles from consent search cases to searches of cyberspace. Nonetheless, I see no reason why the above limitations on consent searches should not apply to protected areas on the World Wide Web. If lines of consent can be drawn in physical space, there is no reason why similar lines cannot be drawn in cyberspace or, specifically, in all the various corners of Facebook. Returning to my hypothetical, if Bernardo shows the Facebook photos of

---

212. 469 U.S. 17, 22 (1984); *see also* United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir. 1971) (holding that consent to search a house for narcotics did not extend to the search of private papers in the home).

213. United States v. Matlock, 415 U.S. 164, 170 (1974) (girlfriend who shared defendant's bedroom could consent to search); Frazier v. Cupp, 394 U.S. 731, 740 (1969) (one of two cousins who shared use of a duffel bag could consent to search). *See* Illinois v. Rodriguez, 497 U.S. 177, 177 (1990) (holding that even when the third party doesn't have actual authority, the search is still valid if the officer reasonably believed that the consenting party had authority).

214. United States v. Padilla, 520 F.2d 526, 527 (1st Cir. 1975).

215. *Id.*

216. *Id.* (citing *Katz*, 389 U.S. at 359-61).

217. 883 F. Supp. 422, 424 (D. Minn. 1995).

Tony's criminal trespass to Officer Krupke, but Officer Krupke commandeers Bernando's laptop and keeps digging further, this would no longer fit into the "plain view" or "consent search" exception. Similarly, if Bernardo only consents to Officer Krupke looking through a Facebook photo album called "Men on Maria's Balcony," such consent would not extend to a different photo album called "Knife-Fighting with the Sharks." Finally, if Bernardo gave Officer Krupke his Facebook account password to use whenever he wanted, such boundless search capabilities should be similarly suppressed.

3. Information Unknowingly Provided to Government Agents

The practice of government officials creating fake online identities to gain access to others' Facebook profiles raises an oft-debated issue: do people have a reasonable expectation that our friends aren't government agents in disguise?

The Misplaced Trust Doctrine suggests that the answer is always a simple "no." In other words, if a Facebook user voluntarily communicates incriminating information to "friends" who are actually moles, narcs, and spies, she has no reasonable expectation of privacy in that information.

However, the myriad ways in which government agents might obtain information through "disguise" on Facebook present different levels of privacy expectations and suggest varying outcomes. To illustrate, here are eight ways that a criminal defendant might unknowingly provide content to the government:

> 1. Defendant's (D) Facebook page is open to the public.
>
> 2. D becomes friends with Steven Pearl (SP), whom D knows to be a police officer.
>
> 3. D becomes friends with SP, whom D knows, but does not realize is a police officer.

> 4. D does not know SP, but accepts his friendship request because they have other mutual friends in common.
>
> 5. D does not know SP, but accepts his friendship because SP purports to be a former classmate or work colleague.
>
> 6. D accepts a friendship request from "SP," his high school best friend. However, D does not realize that "SP" is actually Attorney General Eric Holder, who used SP's photo and biographical data to create a fake Facebook account under SP's identity, for the purpose of gaining access to D's information.
>
> 7. D and SP are good friends. The government hacks into SP's account to view D's information.
>
> 8. After becoming Facebook friends with D through scenarios #3, 4, 5, 6, or 7 above, SP uses Facebook to actively cajole D into committing a crime.

This list is intentionally ordered to begin with examples of passive surveillance and move toward more facilitative operations, which require active involvement and deception by the police.[218]

Scenario 1 is clearly "in plain view," discussed above, and would pose no privacy issues, regardless of whether D was aware that his page was open to the public. Scenario 2 is an even more egregious illustration of someone voluntarily trampling on his privacy expectations.

Scenarios 3 and 4 parallel the futile "I didn't realize that one of the participants in our fight club is actually a police

---

218. For an excellent and more thorough discussion of various surveillance methods, see Elizabeth E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*" 62 STAN. L. REV. 155, 163 (2009).

officer" line of arguments soundly rejected by most courts. As previously discussed, if a person in "real space" conversed with or in front of an undercover agent, courts denied Fourth Amendment protection, reasoning that she should have been more careful about the people with whom she surrounded herself if she expected privacy from government surveillance. In scenario 4, the fact that the undercover officer previously tricked D's friends is of no import. Indeed, in real space, undercover officers typically earn the trust of D's friends in order to earn D's trust. The privacy considerations do not change just because such undercover policing will disproportionately affect those who place too much trust in their friends ("if you're a friend of Mike, you're a friend of mine") or those who regularly accept the friendship requests of random strangers to bolster a façade of popularity.

Scenarios 5, 6, and 7 are more problematic because they involve more active levels of fraud and deceit. For example, if defendant receives a request from a person claiming to be his good friend "Steven J. Pearl" (whom he knows is not a government agent) and Mr. Pearl's profile includes specific information (e.g., his photo or biographical data) that allows him to verify that he has the right Steven J. Pearl, he has a reasonable expectation that he is not communicating with a government official. However, as discussed above, courts have been steadfast in refusing to exclude information obtained from undercover agents.

Moreover, because the Internet naturally invites a healthy skepticism with regard to others' true identity, courts will be especially unlikely to protect information obtained through undercover policing. Indeed, on Facebook, you never know whether a friendship request from "Jenny Taylor" is from the woman you met at last night's party, or from your fraternity brothers who are hoping to play a cruel joke on you. Even though identity theft or hacking is a crime, most courts have nonetheless upheld police tactics that involve violating rules in order to enforce them.

Under existing law, the only scenario that might pose problems under current law is 8. But there, the issue is one of

entrapment, which provides a potential defense to the crime, and not grounds to exclude evidence.[219]

Interestingly, the misplaced trust doctrine only seems to run in one direction. If a user's "friend" turns out to be an undercover agent who violated Facebook's policies to create a fake account, the user has no privacy protections. However, the misplaced trust in the identity or accuracy of any evidence on Facebook has yet to lead to the successful suppression of such evidence.

4. Information Voluntarily Disclosed by Facebook

If Facebook or its employees were to voluntarily provide a user's personal information to government investigators, the Fourth Amendment would not clearly prevent or exclude such evidence under the Voluntary Disclosure Doctrine.

If Facebook's privacy policy clearly stated that it would not disclose information to government investigators unless it received a warrant or subpoena, perhaps users might be able to present a different argument.

But as discussed in Part I of this Article, Facebook's privacy policy as of April 22, 2010 states that:

> We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other

219. For a discussion of how most instances of police surveillance do not constitute entrapment, see Jerome H. Skolnick, *Deception by Police*, 1 CRIM. JUST. ETHICS (1982).

> illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.[220]

The policy clearly states that Facebook will comply with mere "requests," suggesting a standard far lower than reasonable suspicion. The "required by law" part of the first sentence might be interpreted to mean that it will deny any "requests" unless it will face obstruction charges, contempt fines, or other consequences as a result of denying the requests. However, the remainder of the policy makes clear that Facebook reserves the right to hand over any content that might be "necessary to prevent . . . illegal activity."

5. Information Obtained by the Government through Warrants, Subpoenas, or Improper Means

If the Third Party Doctrine is literally applied to all communications on the Internet, Facebook users will struggle to persuade a court that any expectations of privacy are reasonable, even when employing the most restrictive privacy settings. When users interact with Facebook, they should know that an employee of Facebook may view or do something with that information. Moreover, Facebook's privacy policies notify Facebook users that their content may be shared with Facebook's commercial partners; any targeted advertising serves as regular reminders of this fact. Thus, users are on notice that their content can be shared by multiple third parties without any notification.

Most courts would conclude that the reasonableness of a Facebook user's expectation of privacy incrementally diminishes with each additional "friend" who can access the content. Such a rule poses serious problems because content shared via Facebook is less likely to be viewed by only a small,

---

220. *Facebook Privacy Policy*, *supra* note 26.

trusted group of friends, relative to content sent through e-mail. Given the primary purpose of social networking, I would guess that most Facebook users' pictures, status updates, and feeds can be accessed by their entire circle of "friends," which often include people who might better be described as acquaintances, former classmates, and complete strangers with similar interests or romantic potential.[221] In contrast, most people do not send e-mails to their entire address book[222] unless announcing new contact information or forwarding messages about a cash reward from Bill Gates for testing Microsoft's e-mail tracking system.[223] Which is to say, the very purpose of Facebook runs at odds with this privacy rule.

If, then, the current law supports the warrantless and subpoena-less search of a user's *private* Facebook account, this is likely to be at great odds with what most people today would generally consider to be private. When Christopher Slobogin and Joseph Schumacher conducted a survey of individuals to rate the intrusiveness of certain types of searches or seizures on a scale of 0 (nonintrusive) to 100 (extremely intrusiveness), the monitoring of a phone for thirty days rated at a whoppingly high 87.67, only a few points short of the highest-rated search, a body cavity search at the border, which earned a 90.14 rating.[224]

---

221. I am only reaching this conclusion anecdotally and through my own experiences. As discussed above, I am aware that Facebook allows for different types of communications such as e-mail and chatting, which are intended to reach a much smaller subset of individuals. Moreover, I am aware that if a user were to upload a picture or write a rant on her wall, she could also limit which of her friends can see that information. However, I imagine that most users, like myself, do not use Facebook to share information with only a small fraction of their "friends."

222. Initially, I considered using the word "Rolodex" here instead of "address book." However, out of sensitivity to those born in the last quarter century, I have refrained from using such dated terms.

223. *See Microsoft/AOL Giveaway*, SNOPES.COM, http://www.snopes.com/inboxer/nothing/microsoft-aol.asp (last visited Nov. 11, 2010).

224. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 Duke L.J. 727, 737 (1993).

V. Facebook Privacy under Federal Statutory Privacy Laws

In addition to the restrictions of the Fourth Amendment, federal electronic surveillance law in the United States is also governed by the Electronic Communications Privacy Act of 1986 (ECPA),[225] which was, at the time, a forward-looking congressional statute that amended the Wiretap Act of 1968 and specified new privacy standards for emerging and dramatically advancing technologies.[226] Unfortunately, Congress has not significantly revised the statute since 1986, a time when Facebook CEO Mark Zuckerberg's concept of posting on walls involved fewer servers and more crayons.[227]

More specifically, Congress sought to restrict unauthorized surveillance of electronic communications and use ECPA to fill in gaps left by the existing constitutional and statutory framework at that time.[228] In 1986, existing Fourth Amendment doctrine did not protect e-mail and other electronic communications.[229] This remains largely true today.

---

225. 18 U.S.C. § 2511(1) (2000).

226. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. A report by the Office of Technology Assessment suggests that, in 1986, electronic surveillance was no longer limited to telephone taps and concealed microphones, but also included "miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and a rapidly growing array of computer-based surveillance techniques." OFFICE OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 9 (1986). The report also noted that those with enough money, tech savvy, and determination could monitor electronic communications sent via wire, coaxial cable, microwave, satellite, and fiber optics. *Id.* Although encryption prevented such electronic surveillance, such technologies were too expensive and cumbersome for widespread usage in 1986. *Id.*

227. Mark Zuckerberg was born in 1984.

228. S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

229. *See* Zwillinger & Genetski, *supra* note 139, at 574 ("[The law governing subpoenas of electronic communication] was conceived at a time that pre-dated the World Wide Web, and therefore did not contemplate the ubiquitous use of web-based communications services such as Hotmail, Yahoo!, MySpace, or Gmail, and the accompanying copious, long-term storage offered by such providers."). Moreover, as discussed above, the Court's current Fourth Amendment doctrine still does not clearly protect electronic communications that are handled by third-party ISPs.

Thus, the ECPA provides protections that go beyond traditional Fourth Amendment rules. Most notably, under the ECPA, a private ISP cannot invoke the voluntary disclosure doctrine, the private search and seizure doctrine, or the misplaced trust doctrine to protect it from liability. However, the ECPA was also written to allow law enforcement, in limited circumstances, to compel disclosure of electronic communications by meeting various procedural safeguards.[230]

The ECPA divides up communications into three categories—(1) wire communications, (2) oral communications, and (3) electronic communications—and protects each of them differently. These categories could be covered by more than the three distinct parts of the ECPA that provide possible application to searches on Facebook and on the Internet generally: (1) the Wiretap Act, (2) the Stored Communications Act (SCA),[231] and (3) the Pen Register Act. These are discussed, in turn, below.

A. *The Wiretap Act*

The federal Wiretap Act, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, covers wire communications.[232] While it originally only covered wire and oral communications, the ECPA amended it to also cover electronic communications. For those who did not religiously watch *The Wire*, the Wiretap Act broadly prohibits wiretaps,[233] but allows law enforcement to "intercept" communications for up to thirty days (1) upon demonstrating probable cause to believe that the interception will reveal evidence of specific felony offenses, (2) when authorized by the Justice Department, and (3) signed by a federal judge.[234]

---

230. *See* S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

231. *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 3555.

232. 18 U.S.C. §§ 2510-2522. While this statute is sometimes referred to as Title III, I am referring to is as the Wiretap Act since that is the more descriptive and unique name and, besides, I am reserving "Title III" as the first name for my next child.

233. *Id.* § 2511(1).

234. *Id.* §§ 2516-18.

Section 2501(1) of the ECPA defines a "wire communication" as an "aural transfer" that travels through wires or similar mediums. These wire communications generally receive the most protection. Under § 2510(2), an "oral communication" is a communication "uttered by a person exhibiting an expectation such communication is not subject to interception under circumstances justifying such expectation."

But if Facebook communications are covered by this statute, they will fall into the third "electronic communication" category. The ECPA defines this as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," that isn't a wire or oral communication.[235]

Congress intended "electronic communication" to function as a catch-all category.[236] The legislative history reveals that it was intended to include those communications "neither carried by sound waves nor . . . characterized as one containing the human voice (carried in part by wire)."[237] Thus, almost all Facebook communications would qualify as electronic communications.[238]

Undoubtedly, the Wiretap Act provides strong protections for virtually all electronic eavesdropping and requires any exceptions comply with standards even tougher than what the Fourth Amendment requires.

However, the Wiretap Act has questionable applicability to most communications on Facebook because it only covers *interceptions* of electronic communications. Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any contents of any wire, electronic, or oral

---

235. *Id.* § 2510 (12).

236. *See* United States v. Herring, 993 F.2d 784, 787 (11th Cir. 1993).

237. H.R. Rep. No. 99-647, at 35 (1986).

238. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) (electronic communication includes a digital document file transmitted from a web server); *In re* Application of United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006) (holding that electronic communication "is broad enough to encompass email communications and other similar signals transmitted over the Internet").

communication through the use of any electronic, mechanical, or other device."[239] While the statute does not require that the communications are intercepted contemporaneously with their transmission, the design of the SCA, discussed infra, suggests that the Wiretap Act includes such a contemporaneous requirement to avoid simultaneous coverage by two different statutes with different procedures. Moreover, when the ECPA was passed, the concept of "wiretaps" was largely limited to the eavesdropping of a live two-way exchange between two parties.

Most courts that faced this issue have held that the Wiretap Act's coverage of "interceptions" is limited to when the government acquires electronic communications contemporaneously with their transmission.[240]

However, refusing to follow its sister circuits,[241] the First Circuit interpreted the Wiretap Act in such a way that it may have broader applicability to Facebook communications. In *United States v. Councilman*, the court stated that the contemporaneity requirement "may not be apt to address issues involving the application of the Wiretap Act to electronic communications."[242] Specifically, it held that e-mail messages are "intercepted" when acquired while in "transient electronic storage that is intrinsic to the communication process."[243] Thus, in the First Circuit, an electronic communication could be in

---

239. 18 U.S.C. § 2510(4) (2006).

240. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3rd Cir. 2003) (holding that the Wiretap Act did not cover access to stored e-mail communications); United States v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003) (files stored on hard drive); *Konop*, 302 F.3d at 876-79 (website); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-63 (5th Cir. 1994) (stored e-mail communications); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1279 (D. Kan. 2007) (numbers stored in cell phone); United States v. Jones, 451 F. Supp. 2d 71, 75 (D.D.C. 2006) (text messages); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (pager communications); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (same).

241. I have not been able to confirm whether the other federal circuit courts of appeal are sister circuits or brother circuits due to various privacy laws protecting medical records.

242. United States v. Councilman, 418 F.3d 67, 79-80 (1st Cir. 2005) (en banc) (citing *In re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 21 (1st Cir. 2003)).

243. *Id.* at 85.

"electronic storage" while also being in transmission,[244] so long as the acquisition is not "made a substantial amount of time after material was put into electronic storage."[245]

Notwithstanding the First Circuit's rule, most Facebook communications are unlikely to be protected by the Wiretap Act because most aspects of Facebook are designed to be a storage site for communications, and not a conduit for simultaneous conversations. For example, when A posts a message on B's Facebook wall, B does not need to be logged on to receive it. Moreover, the message remains there indefinitely until B actively removes it.

There is currently one aspect of Facebook's communication tools, however, that could be fairly interpreted to fit under the Wiretap Act. Most notably, the chat function on Facebook functions like an "instant messaging" service that typically functions in real-time, like a telephone or face-to-face conversation. Thus, if the government were to set up a cloned Facebook account to monitor a conversation as it happens, the Wiretap Act would apply.

However, as a practical matter, the government is unlikely to seek such surveillance because investigators could circumvent the high procedural hurdles presented by the Wiretap Act by simply waiting long enough to avoid the contemporaneity requirement and then retrieving the same information. After all, unlike telephone calls, telegrams, faxes, and letters, the content of Facebook communications remains on a third party server even long after they have been received by the intended recipients. Chat messages remain archived in the same way as any other e-mail messages.

Presently, Facebook's chat function does not allow video or webcam conversations that are currently available through instant message services provided by Skype, Google, Yahoo! Messenger, or Apple's iPhone. Were this predictably to become a new Facebook feature, the analysis here would not change unless Facebook did not record, archive, or otherwise capture the video transmissions and guaranteed this in its privacy

244. *Id.* at 79.

245. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 21 (1st Cir. 2003).

policies.[246]

Despite the clear need to update the statute, the only current efforts to revise this statute involve proposed legislation that would require all communications services "including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype" to ensure that they will be ready to comply with a government wiretap order.[247]

B. *The Stored Communications Act*

Whereas the Wiretap Act covers transmission, communications in storage are protected by the Stored Wire and Electronic Communications and Transactional Records Access Act ("Stored Communications Act" or "SCA"), which is Title II of the ECPA.[248] "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."[249]

Modeled after the Right to Financial Privacy Act,[250] the

---

246. Given the incredible strain on its servers, most video chat services probably do not record live video conversations. But this is more likely a technological limitation and not a privacy accommodation. Indeed, the privacy policies by these web cam services do not clearly exclude the video content from monitored content and, in fact, write their privacy policies to potentially encompass such content. *See, e.g.*, *Skype Privacy Policy*, SKYPE, http://www.skype.com/intl/en-us/legal/privacy/general/ (last visited Nov. 11, 2010).

247. Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N. Y. TIMES, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&emc=na.

248. 18 U.S.C. §§ 2701-2712 (2006). Like 2Pac, the SCA has assumed many different names. *See* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (2004). I agree with Kerr that it is "easiest and simplest to refer to the statute as simply the Stored Communications Act, or 'SCA.'" *Id.*

249. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008) (citing Kerr, *supra* note 248, at 1209-13).

250. *See* Seth Rosenbloom, *Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act*, 39 COLUM. HUM. RTS. L. REV. 529, 551 (2008). The Right to Financial Privacy Act (RFPA) prohibits banks from releasing financial records without government process. *Id.*

SCA creates civil liability for one who:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[251]

The definition of "electronic storage" in the SCA mirrors the definition from the Wiretap Act:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communications service for purposes of backup protection of such communication.[252]

In essence, the SCA forbids government access to stored contents on third party servers.

However, the SCA also lists a number of exceptions to the disclosure ban, including disclosures to a law enforcement agency under certain circumstances.[253] Section 2702(b) announces a number of exceptions to the general rule of

---

However, the RFPA allows for voluntary disclosures when a bank possesses information relevant to a possible violation of a statute or regulation. *Id.* This information "may include only the name or other identifying information concerning any individual, corporation, or account involved in and the nature of any suspected illegal activity." *See id.* (quoting 12 U.S.C. 3403(c) (2000)).

250. S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

251. 18 U.S.C. § 2701(a) (2000).

252. *Id.* § 2510 (17).

253. *Id.* §§ 2702(b)-(d), 2703.

nondisclosure.[254] Most notably, 2702(b) allows service providers to disclose the contents of electronic communications:

> (7) to a law enforcement agency—
>
> (A) if the contents—
>
> (i) were inadvertently obtained by the service provider; and
>
> (ii) appear to pertain to the commission of a crime; or
>
> (B) [Deleted]
>
> (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

More importantly, section 2702 also provides an exception for disclosures pursuant to a court order under the procedures of 18 U.S.C. §§ 2516 and 2703.[255]

Section 2703 delineates the procedural requirements that the government must meet before it can access various electronic communications.[256] This section provides the greatest protection to the content of communications in "electronic storage" for 180 days or less; this data can only be disclosed through a search warrant supported by probable

---

254. *Id.* § 2702(b).

255. S. Rep. No. 99-541, at 37–38 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3581–82. 18 U.S.C. § 2516 lists the procedures for authorizing an interception of wire, oral, or electronic communications. 18 U.S.C. § 2703 lists the rules the government must meet before accessing electronic communications in storage and transactional records related to these communications.

256. 18 U.S.C. § 2703 (2000).

cause. [257] However, for communications stored for more than 180 days, the government can compel disclosure by obtaining a search warrant, by combining "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" with prior notice to the subscriber or customer, or by combining prior notice to the subscriber or customer with a court order authorized by 18 U.S.C. § 2703(d).[258]

A section 2703(d) order seems to be the love child of a subpoena and search warrant, although it has inherited more of the subpoena's traits. Under § 2703(d), the government must offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[259] This "reasonable suspicion" standard is lower than the "probable cause" requirement of both the Fourth Amendment and the Wiretap Act.[260]

Thus, at the end of this statutory treasure hunt, § 2703(d) of the SCA allows the government to compel Facebook to disclose all content specific to named individuals with a subpoena, without probable cause, and without any meaningful notice. While Congress arguably intended the SCA to avoid this exact scenario,[261] a faithful textual reading of the statute places Facebook users (and all other Netizens who "store" content on ISPs) on the wrong end of the plank.

For Facebook users expecting privacy, the SCA is also woefully inadequate in that it seems to not protect, at all, a large category of content that one receives and shares on Facebook. The vague definitions of "electronic storage" under § 2510(17) and § 2511 leave unclear whether the SCA will protect previously-read communications less than 180 days old

257. *Id.* § 2703(a).

258. Kerr, *supra* note 248, at 1219 (referring to a court order authorized by 18 U.S.C. § 2703(d) as a "Section 2703(d) order").

259. 18 U.S.C. § 2703(b) (2000).

260. *Id.* § 2703(b).

261. *See also* Kerr, *supra* note 248, at 1219 (referring to a court order authorized by 18 U.S.C. § 2703(d) as a "Section 2703(d) order").

stored on an ISP.[262] This is especially alarming since most Facebook content less than 180 days old will fall into this category. First, all Facebook content is stored on a third-party ISP.[263] Second, once a Facebook user logs in, any content on the user's "home page"—i.e., her friend "feed"—may be considered "read," even though the user may not have clicked anything to affirmatively read the message and may not have noticed the communication. Third, content on Facebook does not disappear unless the user actively deletes it, which, unlike e-mail, is not a standard practice.[264]

Indeed, at least three courts that faced this issue interpreted § 2510's definition of "electronic storage" narrowly and refused to extend the SCA's strongest protections to previously opened electronic communications.[265] However, three other courts have interpreted § 2510's definition of "electronic storage" broadly and extended the SCA's strongest protections to e-mails that have been opened and read by the message's intended recipient.[266]

---

262. *See* 18 U.S.C. §§ 2510, 2711 (2002 & 2009).

263. Facebook does not function like a POP e-mail account where one "downloads" content and thereby removes it from a server. While Facebook may send messages or notifications to an inbox that is downloaded to one's hard drive or send a "push" notification to one's smartphone, no content is ever removed from Facebook as a result of this process.

264. Indeed, those who notice that a Facebook user has deleted a photo, message, link, or connection may assume that the user was trying to hide something.

265. *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff'd in part, vacated in part, and remanded by* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) (holding that received e-mails are not protected by the SCA); United States v. Weaver, No. 09-30036, 2009 WL 2163478 (C.D. Ill. July 15, 2009) (holding that e-mail messages on the web-based Hotmail e-mail program are only subject to the SCA's weaker privacy protections); Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008) (holding that read messages retained by the service provider are subject to the SCA's weaker protections for remote computing services).

266. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-76 (9th Cir. 2004) (holding that § 2510(17)(B) protects messages remaining on an ISP's server even after those messages have been delivered to and read by the intended recipient); *In re* Subpoena Duces Tecum to AOL, 550 F. Supp. 2d 606, 614 (E.D. Va. 2008) (holding that the SCA protects non-party witnesses' stored e-mails on AOL).

In *Crispin v. Christian Audigier, Inc.*,[267] a district court judge quashed subpoenas served on Facebook in a copyright infringement lawsuit that sought private messages sent through the site.[268] The court held that such messages were protected information under the SCA because the user employed private settings on Facebook, thereby removing them from the category of public communications.[269] However, the court only addressed one aspect of restricted communications on Facebook—the private messaging that functions like an e-mail service.

Thus, under the SCA, the only Facebook content that the government must *clearly* have probable cause to obtain is "unopened" communications sent within the last 180 days. That is it.

Worst of all, the SCA expressly leaves out exclusion as a remedy when the government obtains content in violation of the statute. Section 2708 states that damages "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."[270] Thus, even if the government obtained information in violation of the SCA, the statute does not prevent its inclusion as evidence in a criminal proceeding.[271]

Even if a defendant could successfully challenge the constitutionality of the compelled disclosure rules of § 2703's procedures, federal precedents strongly suggest that suppression would not be a proper remedy so long as the evidence was obtained in objectively reasonable reliance on the statute. For example, in *Illinois v. Krull,*[272] the Supreme Court

267. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

268. *Id.* at 991.

269. *Id.*

270. 18 U.S.C. § 2708 (1986).

271. *See* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) ("violations of the ECPA do not warrant exclusion of evidence"); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998); United States v. Ferguson, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000); United States v. Reyes, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996).

272. 480 U.S. 340 (1987)

considered the admissibility of evidence obtained pursuant to an unconstitutional state vehicle code.[273] The Court held that the exclusionary rule should not suppress evidence "obtained by an officer acting in objectively reasonable reliance on a statute."[274] While the Court left open the possibility that exclusion would be appropriate for a "clearly unconstitutional" statute,[275] there is no reason to think that § 2703 fits into that category. The only federal decision that held § 2703's procedures unconstitutional was later reversed on appeal.[276]

The possibilities to circumvent the SCA's restrictions are numerous. The SCA is limited to the government and, thus, does not prevent Facebook or Internet service providers, in any way, from accessing stored data.[277] Moreover, if private parties were to seek access to Facebook content through civil discovery, the SCA is unclear on whether exceptions are made for disclosure requests pursuant to a civil discovery subpoena.[278] Thus, if non-government authorities were to access Facebook communications, there would be nothing stopping those private agents from handing over any information to government investigators.

Finally, in the context of analyzing Facebook users' rights under the SCA, perhaps the most important statutory interpretation is not one from any court, but rather from Facebook's own practices. As mentioned above in the discussion of the Justice Department's memorandum obtained by the EFF, Facebook makes "other data available" and is "cooperative with emergency requests,"[279] while "MySpace requires a search warrant for private messages/bulletins less than 181 days old" and "considers friend lists to be stored

---

273. *See id.* at 343-44.

274. *Id.* at 349.

275. *Id.*

276. *See* Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc).

277. *See* 18 U.S.C. § 2703(c)(1) (2009).

278. At least one federal court held that civil discovery subpoenas do not fit within the statute's recognized exceptions allowing for the disclosure of electronic communication. *See In re* DoubleClick, Inc., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001).

279. John Lynch & Jenny Ellickson, *supra* note 80, at 17.

content."[280]

While the document does not state that Facebook's policy is different from MySpace's procedures, Facebook has informed attorneys with subpoenas in civil cases that "if the requesting party is a governmental agency, a search warrant is required for private inbox and/or outbox communication 180 days old or less. See 18 U.S.C. § 2703(a)."[281]

Assuming that remains Facebook's policy, this is clear evidence that Facebook does not require warrants for any content more than 180 days old and only requires it for private messages.

C. *The Pen Register Act*

The Pen Register Act[282] (PRA) authorizes the government to seek a court order authorizing a (1) "pen register," which records outgoing address information[283] or (2) a "trap and trace device," which records incoming address information.[284] The constitutionality of the statute stems from *Smith v. Maryland*, which was discussed above. However, the statute provides a smidge more protection than that offered by the Fourth Amendment.

To obtain either a pen register, a trap and trace device, or both, the government must certify that "the information likely

---

280. *Id.* at 22.

281. Sam Glover, *Subpoena Facebook Information*, LAWYERIST, (July 10, 2009), http://lawyerist.com/subpoena-facebook-information/.

282. 18 U.S.C. §§ 3121-3127 (2010). Others have referred to this portion of the statute as the Pen/Trap Statute. I will not be using that term, however, so as not to create confusion between other laws regulating snares used to catch writing instruments.

283. The PRA defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(3).

284. The PRA defines a "trap and trade device" as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(4).

to be obtained is relevant to an ongoing criminal investigation."[285] The standard suggests something far lower than probable cause and, perhaps, even lower than reasonable suspicion, since the government need not even state any specific facts to obtain the order. Moreover, the PRA does not require the government to either report back what they intercepted or notify the surveillance targets that they were monitored.

The PRA applies to computer network communications.[286] With regard to Internet communications, because most Internet headers contain both the "to" and "from" information, a device that reads such headers is often referred to as a "pen/trap device."

If a pen/trap is served on an Internet service provider, the information recovered pursuant to the PRA must be limited to non-content information such as a user's "dialing, routing, addressing, [and/or] signaling information" and e-mail account. Thus, the PRA likely permits the government to obtain:

> - All e-mail header information, including the address recipients, the time sent or received, and the size of the e-mail—but not the subject line
>
> - The IP addresses involved
>
> - The communications ports and protocols involved[287]

One unanswered question is whether these pen/traps allow the government to obtain the URLs of every website visited. On the one hand, a web address is analogous to a mailing address or a telephone number, both of which are not traditionally

---

285. *Id.* § 3122(b)(2).

286. *In re* Application of United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006).

287. Unfortunately, my understanding of the technology behind communications ports and protocols is about as limited as my vocabulary in Aramaic. However, after putting in inquires with all of my computer science friends, both of them replied that this information would reveal what applications were used to send the communications.

protected under the Fourth Amendment. Moreover, learning that a person visited http://neuticles.com does not reveal any more information than learning that a person called 888-638-8425, which is the toll-free line for ordering canine testicular implants from the Neuticles company. On the other hand, addresses like http://inmatesforyou.com or http://en.wikipedia.org/wiki/List_of_ancient_Jedi suggest far more content than would be obtained by phone numbers.

This question of the admissibility of URL addresses is especially important in the context of Facebook. After all, if a Pen/Trap revealed that a Facebook user visited http://www.facebook.com/pages/When-someone-says-stop-my-brain-says-Hammertime/203249412335, the information revealed goes far beyond the traffic analysis originally envisioned by the statute. Because of the way that URLs on Facebook are named, the police would not only learn IP addresses and sizes of communications, but also an intimate secret that the investigated individual may possess—that when he hears, "Stop!", his brain often says, "Hammertime!"

Another unanswered question of law is what happens when the government cannot use a pen/trap device without collecting impermissible content. There are at least two district court decisions suggesting that these devices cannot be used if it collects content.[288] Finally, a related emerging issue is whether the PRA authorizes the collection of "post-cut-through dialed digits," which is a questionably-worded term to describe those numbers dialed after an initial call is complete.[289]

---

288. *See In re* Application of the United States, 622 F. Supp. 2d 411, 422 (S.D. Tex. 2007) ("[T]he Pen Register Statute does not permit the Government simply to minimize the effects of its collection of unauthorized content, but instead prohibits the collection of content in the first place."); *In re* Application of United States, 416 F. Supp. 2d at 17 ("[T]he Government must ensure that the process or device used to obtain information about e-mail communications excludes the contents of those communications.").

289. The few courts that faced this issue held that the pen/trap devices cannot be used if they collect these post-cut-through dialed digits. *See In re* Applications of United States, 515 F. Supp. 2d 325, 339 (E.D.N.Y. 2007); *In re* Application of United States, 622 F. Supp. 2d. at 422; *In re* Application of United States, 441 F. Supp. 2d 816, 827 (S.D. Tex. 2006). While post-cut-through dialed digits do not literally pertain to the Internet or Facebook, I mention it here for two reasons. First, whatever rules ultimately emerge will affect what happens when a pen/trap device collects similarly extraneous

D. *Summary of Facebook Privacy Rights under the ECPA*

Under the ECPA, as interpreted by the courts, the Justice Department, and Facebook, the only Facebook content *clearly* protected by the statute are "unopened" e-mails sent within the last 180 days, which requires the government have probable cause to obtain. There is an active dispute over whether "opened" e-mails sent within the last 180 days are also similarly protected. Nothing else clearly requires a warrant.

Beyond private Facebook messages less than 181 days old, all other content can be disclosed with a mere subpoena and no notice. Moreover, the subpoena may not even be required for content that is arguably outside the scope of the ECPA like friend lists, which are not clearly "communications" that are stored or "content" in transit. Finally, if the government compels disclosure without fully meeting the subpoena or warrant requirements, the ECPA provides no suppression remedy to exclude the improperly-obtained evidence from being used against a criminal defendant.

Even if the ECPA is interpreted to protect more Facebook content and apply the warrant requirement to that content, Facebook is still not prevented from voluntarily disclosing its users' content to the government. Its privacy policies are too vague to provide users with an argument that disclosures of criminal activity violated the terms of the agreement.

VI. Facebook as the Twenty-First Century Phone Booth: A Proposal to Redefine Reasonable Expectations and Revise the ECPA

One of the many flaws in federal privacy laws can be most easily summarized by considering the following two facts:

---

content information from a Facebook user. Second, I strongly suspect that the framers of the Fourth Amendment clearly intended to protect the government from obtaining the identities of the specific dancers that my wife and I vote for, using a touch-tone phone, on the reality dance competition show, *So You Think You Can Dance*. However, as of yet, neither I nor the editors of the *Pace Law Review* have been able to obtain any support for this assertion.

> 1. All Facebook users lack a reasonable expectation of privacy if Facebook openly admits that it monitors its users' content and activity.
>
> 2. Facebook polices its site and users for sex offenders and other related suspicious activity.

I am relieved and grateful that Facebook is proactively making Facebook a safer space for minors. But Facebook cannot engage in such protections without also trampling upon my privacy rights. The only reason that privacy and a predator-free Facebook are mutually exclusive, however, is because of judicial opinions written before online social networking sites surfaced.

First and foremost, I submit that *Katz* should be interpreted in ways more focused on the Court's concern about the parameters of government surveillance and less focused on whether an individual expects privacy from non-government entities.[290] The Court suppressed the content of Katz's phone conversation even though he stood in "public," in full view of others, and knowingly divulged the "content" of his message to another citizen, as well as all the operators that had the capability to listen in.[291] That the person to whom he was speaking or the eavesdropping operators could have divulged the content of the call to others did not affect the outcome.

There is at least one meaningful difference between Katz's 1967 conversation in the phone booth and the equivalent one

---

290. *See, e.g.*, Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125 (2002). My thoughts were influenced by an article written before *Katz* by Anthony Amsterdam, who asked whether the Fourth Amendment should "be viewed as a collection of protections of atomistic spheres of interest of individual citizens or as a regulation of governmental conduct[?] Does it safeguard *my* person and *your* house and *her* papers and *his* effects against unreasonable searches and seizures; or is it essentially a regulatory canon requiring government to order its law enforcement procedures in a fashion that keeps us collectively secure in our persons, houses, papers, and effects, against unreasonable searches and seizures?" Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 367 (1974) (emphasis in original).

291. Katz v. United States, 389 U.S. 347, 351 (1967).

he might have on Facebook today. Today, Katz would be having more of a "party line" conversation on Facebook, whereas he was presumably only talking to one individual in 1967. While this might suggest that a Facebook user who broadcasts his status to his one thousand friends is *less* likely to have a reasonable expectation of privacy, the Court never suggested that additional message recipients instantly defeat the expectation. There is no language in the opinion to suggest that had the bookie, whom Katz called, asked a colleague to pick up another telephone in the house to form a three-way conversation, the outcome would have changed.

As the Court in *Katz* stressed, the question of what "may be constitutionally protected" depends on what a person "seeks to preserve as private."[292] Thus, the fact that Katz was standing in a glass Los Angeles telephone booth, as opposed to his private home, did not defeat his right to be free from government surveillance. His act of "shut[ting] the door behind him" was the action he took to indicate that he did not intend to "broadcast to the world."[293] The fact that the person whom Katz was calling could have broadcast the content to the world did not even warrant mention in the majority opinion.

Courts should view Facebook as the twenty-first century equivalent of a phone booth. Just as the "question is not whether the telephone booth is a constitutionally protected area,"[294] the question should not be whether Facebook is or is not a constitutionally protected area. Today, if Katz's son sets his Facebook content to "private" and limits his conversations to trusted friends, he has done the equivalent of shutting the phone booth doors. As discussed above, he cannot possibly expect that his content will be kept out of the government's hands—whether because of friends sharing the information, Facebook forwarding the information, or because the government could obtain a warrant—just as Katz could not assume that the person he called would not divulge the content of the conversation to the police.

However, he can reasonably assume that he is not

292. *Id.* at 351.
293. *Id.* at 352.
294. *Id.* at 349.

undergoing government surveillance despite the fact that: (1) a Facebook employee can "listen" to the conversation (just as a telephone operator could do the same); (2) he has no way of knowing who, exactly, is on the "other line"; and (3) he knows that his content might be seen beyond the intended distribution list (just as Katz's bookie could have invited government agents to come over and listen in on the call).

Conversely, a Facebook user who keeps his setting "public" has left the phone booth door open and sacrificed his privacy protections, even if communicating from home. That user knows that what "he utters into the mouthpiece" will "be broadcast to the world."[295] Moreover, the information that is always public on Facebook—one's profile photo, for example—is equivalent to one's physical appearance or clothes while standing in a glass phone booth. There can be no expectation of privacy there since a government investigator could snap a photo at any moment. Finally, the IP address is an example of non-content information on par with a telephone number.

The shift toward interpreting *Katz* as an opinion about limiting government surveillance—and less about individual rights—may not be of much import in most criminal procedure contexts. Such a shift would not affect whether local police should be able to enter individual homes to search through one's hope chest or dream journal. But that shift would allow social networking sites to allow users to communicate without giving up their rights against unwarranted government surveillance. After all, if the Fourth Amendment solely protects the "atomistic spheres of interest" of an individual, then privacy no longer exists when two individuals connect through Facebook.[296]

This shift would also effectively redefine the Third Party Doctrine to focus on whether a third party who works for the government has access, not on whether *any* third party has access. This shift is necessary since in today's digital age, other companies such as Internet service providers and Facebook, will be able to access both content and non-content information. Even if Facebook has a license to distribute its users'

295. *Id.* at 352.

296. Amsterdam, *supra* note 290, at 367.

intellectual property, it does not own the information. Facebook is merely a steward of this information. Thus, there is nothing inherent to joining Facebook that should be seen as sacrificing all privacy interests.

In that context, I find the Court's decision in *Miller* addressing bank records to be instructive. In the same way that a bank customer might consent to a bank employee viewing her "private papers," a Facebook user effectively consents to Facebook employees viewing her "private" content. Just as the bank does not own or possess the private papers, Facebook does not own or possess the user's content. Thus, applying *Miller*, courts should be able to separate out the "private papers" from the "business records" on Facebook.

Similarly, if the Fourth Amendment was intended to be a regulation of governmental conduct to preserve society's privacy interests, as I believe, then private communications through a third party social networking site should be just as protected as private communications through the postal service. Just as the sender of a first class letter has a privacy expectation in the content inside the envelope, but not the information outside the envelope, a Facebook user should have an expectation of privacy in the content of her correspondence, but not the routing information for the data.

Thus, when considering the constitutionality of government searches on social networking sites, a court's focus should not be on the user's individual expectation of privacy, but rather, the individual's expectation of privacy from government surveillance. Any other result would lead to a perverted outcome where increasingly archaic communication tools have advanced privacy protections and modern communication tools will lack them.

Nothing inherent to the architecture of the Internet necessitates such a drop in privacy protections. Undoubtedly, in the age of high-definition video cameras that fit into one's pocket, citizens in wired societies understand how much more detailed information can travel much more quickly to many more people. But this reality does not translate to the inevitability of constant surveillance. In fact, with electronic data, a company with resources like Facebook could encrypt data and make privacy expectations higher than any other

form of communication.

If anything, the government's access to advanced technological surveillance tools like KeyLogger, which uses hardware or software to covertly track the keys struck on a computer keyboard so that the government can collect passwords,[297] should be accompanied by similar privacy "upgrades." Otherwise, modern technology will always shift the balance towards government surveillance and away from citizen privacy.

Of course, even if the Supreme Court adopts a "reasonable expectation of privacy from government surveillance" rule, it may not protect users of social networking sites when warrantless government searches become more widespread and publicized.[298] Indeed, one high-profile arrest may be enough to destroy the nation's expectation. If Facebook openly and willingly passes pop singer Justin Bieber's incriminating photos to government investigators who subsequently arrest him for a non-life-threatening crime, the ensuing publicity itself could diminish the nation's privacy rights.[299]

Of course, even if Facebook gleefully provided government investigators carte blanche to view users' information, I suspect the site would still be active, thanks to its millions of users who are law-abiding (and have nothing to hide) or law-ignoring (and want to highlight their rebellious nature) or too curious to cut themselves off from their friends' broadcasts. Put another way, many users may knowingly sacrifice their privacy in exchange for the opportunity to see what their high school prom dates look like a decade later.

But without both governmental and Facebook privacy protections in place, I suspect millions of users will close their

---

297. *See* Declan McCullagh, *Feds Use Keylogger to Thwart PGP, Hushmail*, CNET NEWS, (July 10, 2007, 4:45 AM), http://news.cnet.com/8301-10784_3-9741357-7.html.

298. Or when this Article makes its way to the nightstand of every American, which may or may not be inevitable.

299. The incident could easily shatter expectations of privacy from government surveillance, prompt users to diminish or altogether cease Facebook activity, and require Facebook executives to hire security to protect themselves from angry Beiberbots, Beliebers, and others infected with Bieber Fever.

accounts or stifle their activity upon realizing that their lives may be under government surveillance. After all, even though Facebook users can choose what to share and to whom it will be disclosed, they cannot control what incriminating information will be revealed by their friends or soon-to-be unfriended frenemies. Thus, their best option is to leave Facebook altogether and hope that their absence will prompt their friends to leave as well.

While the stifling of Facebook activity may be inconsequential, the need for a statutory revision is paramount. At stake is nothing less than the potential for the Internet to be a utopian marketplace of ideas and a global community that connects people in an otherwise-isolated digital world.

As for statutory revisions, I propose the SCA be amended to require that any compelled disclosure of electronic information, including content on Facebook, require full warrant protection. This would require the government to demonstrate probable cause to a neutral magistrate. If, however, the government will still be allowed to conduct such searches with an administrative subpoena, the ECPA should require that subpoenas provide meaningful notice to the user to bring the privacy laws closer to the warrantless searches allowed in other contexts. To close these gaping holes in the current privacy laws, Congress must implement several changes.

First, the Stored Communications Act needs to be revised to make clear that all forms of content that a person uploads to or disseminates through Facebook are covered. Given that Facebook reveals "content" that may not neatly fit into the definition of "electronic communications," the statute should leave no doubt that all activity on Facebook—including wall postings, photo-sharing, or event-creating—will be protected. Moreover, in light of all the data that Facebook users provide when joining the site, the specific subscriber information or "non-content" that can be disclosed without any judicial oversight should also be delineated.

Second, the SCA must be amended to require the government to obtain a Section 2703(d) order for all remote computing services (in addition to electronic communications

services). Thus, regardless of whether Facebook is serving as "storage" or as a facilitator of messages, judicial supervision will be required if any content stored on the site will be disclosed to the government.

Third, the SCA should also impose a court-order provision on non-governmental entities that compel production of the contents of electronic communications under § 2703.[300] Without this judicial oversight, the voluntary disclosure doctrine would allow private entities to easily compel such production and hand it over to the government. Moreover, such an amendment would eliminate the conflicting interpretations of the SCA.

Fourth, the SCA should state that the exclusionary rule will apply to evidence obtained in violation of any of these statutory provisions, even if the evidence was not obtained pursuant to a government search under the Fourth Amendment. Without this last component, the SCA, in the

---

300. *See* Zwillinger & Genetski, *supra* note 139, at 597-98. The authors propose the following amendment, which I wholeheartedly endorse:

> "18 U.S.C. § 2702(c)(4): Court orders by non-governmental entities.
> A non-governmental entity who is a party to pending criminal or civil litigation may petition the court in which such litigation is pending for an order requiring a service provider to disclose contents of electronic communications in electronic storage or contents of wire or electronic communications in a remote computing service and such order shall issue only if the requesting party can demonstrate that the requested information is relevant and material to the ongoing litigation and is unavailable from other sources, and both the subscriber or customer whose materials are sought and the service provider from whom the materials will be produced are provided reasonable notice and the opportunity to be heard. In the case of a State court, such a court order shall not issue if prohibited by the law of such state. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature, or compliance with such an order would cause an undue burden on such provider. In all cases, the service provider shall be entitled to cost reimbursement by the requesting party, as set forth in 18 U.S.C. § 2706."

Id.

criminal context, will not extend any privacy protections beyond what the Fourth Amendment already guarantees.

Fifth, to ensure that administrative subpoenas do not lead to unjustified intrusions of privacy on the Internet, federal law should ensure judicial safeguards in the form of a neutral magistrate who protects against over breadth and harassment and requires an explanation as to why a subpoena is necessary. Moreover, if a subpoena will not provide a user with notice and the chance to file a motion to quash, federal laws should limit the issuance of subpoenas to life-threatening crimes in which time is of the essence.

Sixth, Congress should mandate encryption for those government and non-government entities that transmit sensitive or private information through the Internet. Since not all companies have the resources to do this, the government should invest in more advanced encryption technology and other cyber-security measures to ensure the highest safety of sensitive and private content transmitted through the Internet.[301] Under the existing Third Party Doctrine, encryption would increase users' expectation of privacy because Facebook employees would not be able to view all user content. While law enforcement agencies might argue that this will frustrate efforts to crack down on cybercrime (and all other crime), such encryption measures will also minimize the crime or cyberterrorism that results when others with more nefarious motives gain access to such information.

Lest I be accused of fighting for criminals' rights, my concern here is more about the chilling effect that comes with

---

301. According to postings on CNET, one reason websites like Facebook, AOL, Yahoo, and Microsoft do not currently offer encryption to their users is the slightly slower speed at which servers function when using a secure web search and the processor power required to scramble and unscramble the SSL connection. *See* Elinor Mills, *Google Rolls Out Encrypted Web Search Option*, CNET NEWS (May 21, 2010, 12:30 PM), http://news.cnet.com/8301-27080_3-20005636-245.html?tag=mncol;txt. However, users have increasingly demanded encryption options and, in some cases, turned to third party encryption websites and "add-ons" offered through web servers such as Firefox. *See* Elinor Mills, *Firefox Add-On Encrypts Sessions with Facebook, Twitter*, CNET NEWS (June 18, 2010, 2:24 PM), http://news.cnet.com/8301-27080_3-20008217-245.html. While it may be a matter of time before private companies invest in this technology themselves, the government is in the best position to invest in this public good and speed up the process.

secret government surveillance. Much of the "good" that Facebook currently provides—political change, romantic unions, and safe spaces for like-minded individuals to have an outlet for frustrations—would probably be stifled in real space if people knew that government cameras were monitoring their activity.

One illustration of this chilling effect pertains to the interesting relationship that "closeted" gay and lesbian Americans have with Facebook. Imagine a gay man who is "out" to a small group of trusted friends, but wishes to remain "in the closet" to everyone else. The minute he joins Facebook, he faces a tough choice when asked about his sexual orientation: he could lie (and risk being mocked or criticized), he could violate Facebook policies and create two accounts,[302] or he could choose not to reveal his sexual orientation but vigilantly police his Facebook page to ensure that friends do not unintentionally force awkward conversations with family members who think he "just hasn't met the right woman yet."[303] Plus, the more honest he is about other connections and interests, the more he risks being outed; two MIT students developed a software program called "Gaydar" that predicts sexual orientation based on the user's interests and circle of friends.[304] On the other hand, as Queerty blogger Arthur Dunlop observed, "services like Facebook and Twitter are actually also fantastic for closeted queers. They are lifelines to other people like you, with the same fears and anxiety you're

302. Part of Facebook's efforts to crack down on this practice include recent decisions to shut out users with unusual names. Barbara Ortutay, *Real Users Caught in Facebook Fake-Name Purge*, SFGATE, May 25, 2009, http://articles.sfgate.com/2009-05-25/business/20872135_1_accounts-with-fake-names-facebook-facebook-guidelines-and-features. This became a problem when actual users like Robin Kills The Enemy, a Native American woman, was shut out of her account. *Id.*

303. This explains why Joshua Alston of Newsweek advised a friend: "if you want to be in the closet, you can't be on Facebook." Joshua Alston, *The Digital Closet*, NEWSWEEK, June 2, 2010, http://www.newsweek.com/2010/06/02/the-digital-closet.html.

304. *See* Carolyn Y. Johnson, *Project 'Gaydar,'* BOSTON GLOBE, Sept. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

facing living a double life."[305] Clearly, this is a tough personal choice that has motivated some to come out to everyone on Facebook[306] and led others to stay away from social networking altogether.

But now imagine that this man must make this choice in a forum with few limits on government surveillance. Announcing that one is gay is not a crime. But it can lead him to be discharged from the military under Don't Ask, Don't Tell. It can also cost him the opportunity to adopt a child in states like Florida.[307] While the risks exist without government surveillance, he need not be overly suspicious to conclude that he is better off staying away from social networking or living a less honest life online. Such a result, I submit, is antithetical to the philosophical underpinnings of the First and Fourth Amendments.

I should admit that, as a new parent, I worry about crime much more. My son is not old enough to do much more than bang on the keyboard, but I still worry about the ways in which Facebook and the Internet pose additional dangers to children. But even at my most paranoid, I find myself more concerned than comforted by unrestrained police surveillance. Perhaps this is because on Facebook, unlike other sites that allow anonymous postings, the community seems to have developed a strong set of self-policing norms that led to many arrests to which I have no objections.

Finally, I should note that if all of my suggestions are implemented, courts may still conclude that some or all Facebook users lack a "reasonable" expectation of privacy, especially given the company's current policies. A judge may conclude that the very purpose of social networking sites—which is to share information—requires a presumption against

---

305. Arthur Dunlop, *Is It Impossible to Stay in the Closet If You're on Facebook and Twitter?*, QUEERTY (June 3, 2010), http://www.queerty.com/is-it-impossible-to-stay-in-the-closet-if-youre-on-facebook-and-twitter-20100603/#ixzz10kAOyPhU.

306. Caryn Brooks, *How to Come Out on Facebook*, TIME, June 2, 2009, http://www.time.com/time/nation/article/0,8599,1901909,00.html.

307. *See* FLA. STAT. § 63.042(3) (2009) (banning "homosexuals" from adopting); Lofton v. Sec'y of the Dep't of Children and Family Servs., 358 F.3d 804 (11th Cir. 2004) (upholding the law).

privacy. I have no objection to this, so long as the conclusion is reached by exploring the specific facts, contexts, and policies that led the evidence into the government's hands.

My recommendations above are largely intended to prevent a judge from using the following checklist while overseeing a suppression hearing for non-e-mail content:

- Was the evidence obtained from the Internet?

- If yes, do not suppress.

Until this checklist adopts analogous factors used to judge the reasonableness of a user's expectation of offline privacy, the Internet will be dueling privacy until one or both of them dies.

VII. Conclusion

I am not a privacy "nut," despite what this Article might suggest. In fact, I have given up most of my own personal expectations of privacy since the late 1990s, when I accepted that existing in the digital era and enjoying modern technology meant living life in a glass house. But the reasons behind my privacy surrender were not ones that could be shared by everybody. In fact, they were quite specific to me, my age, and my Japanese immigrant parents who named me.

To explain, I must tell you two things about me. First, to my knowledge, there is no other Junichi Semitsu in the world. While Junichi is a fairly common Japanese name, Semitsu is a very unusual name in Japan (and every country that lies north, south, east, and west of Japan).

Second, I was an undergraduate at U.C. Berkeley from 1991-1996. When I was a freshman, only the computer science students had e-mail accounts. But by the time I graduated, every student—even ones majoring in Amish Studies[308]—had

308. So that I do not get accused of defaming my beloved alma mater, I should state, for the record, that there was no official major at U.C. Berkeley called Amish Studies. However, as Berkeley allowed undergraduates to create an Interdisciplinary Field Major that allowed students to customize their own areas of study, I cannot affirmatively say that a student did not

an e-mail account. We students began exploring, communicating, and creating on the new frontier of the Internet, unaware of the immortal digital trail left behind.

Thus, when Yahoo! and Google began indexing the web in the late 1990s, a web search for "Junichi Semitsu" resulted in only sites related to me. Not one indexed page included the words "Junichi" and "Semitsu" for reasons unrelated to me. Unlike the John Smiths and Maria Lees of the world, I had no way to "hide" on the Internet.

As a result, any person on the Internet today can still see, for example, the entire classified ad I posted on a usenet bulletin board in 1995 inquiring whether anybody wanted to buy my extra Lollapalooza tickets to see Beck, Hole, and Cypress Hill perform.[309] At the time, I had no concept that I was writing words that would outlive me and, perhaps one day, allow my great-grandchildren to discover their great-grandfather's college phone number.

Thus, I have accepted that I have no privacy on the Internet. I could hope that sites documenting my nonsensical ramblings or youthful indiscretions will fade when overshadowed by sites about other people named Junichi Semitsu. But for this plan to succeed, I need to procreate like Kate Gosselin and name my kids like George Foreman,[310] or inspire hundreds to change their name to Junichi Semitsu. Given the low probability of either event, my online past will always affect my offline future.

It does not have to be this way for everybody. But the lack of SNS privacy protections will eventually push the young John Smiths and Maria Lees of the world to join me in acquiescing to a life without privacy.

Warning people about privacy risks on Facebook will have the same effect as warning them about the dangers of driving.

---

develop a concentration devoted to studying the Amish.

309. *See* Junichi P. Semitsu, *FS: LOLLAPALOOZA Tix – First Tier – 8/18 – ucb.market.misc*, GOOGLE GROUPS, http://bit.ly/a3GkkH (last visited November 29, 2010). I am grateful that I was not looking to part with my extra New Kids On The Block cassingles.

310. All five of his sons and two (out of five) of his daughters are named George Forman. *See Biography for George Forman*, IMDB, http://www.imdb.com/name/nm0286040/bio (last visited November 29, 2010).

Just as some might be incentivized to use public transportation more, some might be less inclined to document every aspect of their fraternity's hazing rituals. But, like cars, social networking sites like Facebook are not disappearing anytime soon. Thus, like me, they will simply surrender and acquiesce to living life in the open.

Hoping for an SNS with better privacy policies to overtake Facebook's place in the national zeitgeist is equivalent to hoping that crystal meth will motivate an addict to stop using heroin. Granted, under basic marketplace theory, Facebook's troubling privacy practices should prompt users to find another site with better policies or, perhaps, to abandon SNS altogether. More broadly, the lack of privacy on the Internet should motivate users to go offline. But that ignores the reality that, in the twenty-first century, life without the Internet is hardly a life at all.

Facebook is not just an important part of people's social lives. It has become an essential part of our lives. But even if another social networking site with better privacy policies comes along and steals Facebook's traffic, the possibility of constant warrantless surveillance by the government will remain.

One thing that Mark Zuckerberg, the Supreme Court, and I all agree on is that privacy is a "social norm" that "has evolved over time."[311] But while Zuckerberg has essentially declared that privacy is dead,[312] the Supreme Court has not concurred and I remain naively hopeful that he is wrong. If Zuckerberg is correct, however, that privacy as a social norm is dead, the Supreme Court's jurisprudence suggests that our legal privacy rights will follow it to the grave.

This explains why my concerns about Facebook privacy are much bigger than Facebook. If our privacy rights under the Constitution depend on our collective reasonable expectations and the Facebook generation comes to accept life without privacy, the result will inevitably be a nation without privacy.

---

311. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN, (Jan. 11, 2010, 1:58 GMT), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

312. *Id.*

Given my resistance to accept such altered norms and refusal to concede that such shifts should alter our collective privacy rights, I am tempted to suggest that my interpretation of the Fourth Amendment is originalist in nature. Undoubtedly, it's a ridiculous exercise to ask what the Framers of the Bill of Rights might have thought about government surveillance through a global social network on a digital and optical data communication system viewable through the hypertext transfer protocol. (Obviously, James Madison would have immediately joined Facebook just to check out pictures of George Mason's wife.)

But the question is better framed as such: Would the Framers have tolerated the King of England and British customs inspectors conducting unjustified investigations of American citizens through Facebook, as opposed to warrantless searches, if the monarchy's level of access was the same? If Facebook was a government operation and citizens were required to join, the Framers would have pointed their muskets at Mark Zuckerberg.

But would the Framers have accepted similar results merely because a private company managed to lull citizens into sharing their intimate thoughts while voluntarily passing on any incriminating information to the throne? It defies logic to suggest they would have lived under the rule of a government with the largely unchecked ability to monitor the intimate details of private individuals merely because new technology makes such surveillance possible.

In my view, the Fourth Amendment was drafted to create a balance between the government's need to ensure order and the citizen's right to live life without unchecked surveillance into her private affairs. Facebook has fundamentally tilted that balance.

Death will be knocking on privacy's door unless Congress and the courts ensure that Americans be granted online privacy rights on par with those available offline. Without such intervention, privacy may soon be reduced to a Facebook memorial page that allows older users to wax nostalgic and mourn an idea gone too soon.