AS ACTIVISTS, WE MAY WANT TO REACH AS MANY PEOPLE AS POSSIBLE AND GAIN APPROVAL FOR OUR MARGINALISED CAUSES, BUT TOO OFTEN WE LOSE SIGHT OF THE EFFECTS OF THE TOOLS WE USE.

THE FACT THAT PEOPLE SEE SOCIAL MEDIA AS A TOOL FOR SOCIAL CHANGE IS MORE A TRIUMPH OF MARKETING THAN THE RESULT OF SOME DIGITAL REVOLUTION.

SOCIAL MEDIA IS A POWERFUL TOOL FOR THE VERY INSTITUTIONS THAT WE ARE AT WAR WITH

THE PEOPLE THAT SEEK TO EXPLOIT AND OPPRESS US. EMBRACING IT HAS RESULTED IN OUR WILLING PARTICIPATION IN A PROCESS OF SURVEILLANCE THAT WE SHOULD BE ACTIVELY RESISTING.

WHO NEEDS THE NSA WHEN WE HAVE FACEBOOK?

BY EVAN TUCKER

Chapter by:
Evan Tucker

From:
Life During Wartime:
Resisting Counterinsurgency (2013)

Ed.:
Kristian Williams
William Munger
Lara Messersmith-Glavin

Zine-ified by:
Some random activists on unceded Wurundjeri land

Note:
We could not photocopy this book so we have used slightly unconventional means to copy the pages. We tried to make the text as clear as possible!

excerpt:

“social media normalises relentless record-keeping of our lives and tracks us like never before. these sites give governments and businesses access to information that they would never have the time or resources to acquire on their own. it also avoids the scandal associated with the exposure of massive surveillance programs, because the subjects of these “dossiers” [your facebook or instagram page] are the same people who produce and disseminate them.

[…]

“at zachary jenson’s bail hearing, his myspace and livejournal accounts were referenced frequently. a straight-faced prosecutor announced that on jenson’s myspace page he admitted to being a “ninja” and an “assassin,” thus proving that he was too dangerous to be released on bail. the prosecution also used information from jenson’s myspace account to argue he had no residence and no ties to a particular geographic community and was therefore a “flight risk.” no independent corroboration was required for these claims because they were jenson’s own words. jenson was denied bail.”

65 Thomas Fuller, "Main Opposition to Boycott Myanmar Election," *The New York Times*, Mar. 29, 2010.

66 Republican Sinn Fein, "Elections and Abstentionism." *Republican Sinn Fein*. Jan. 22, 2012, http://www.rsf.ie/election.htm.

67 Vagabond Theorist, "Why I Don't Vote," *Infoshop News*, Nov. 2, 2010.

68 Dahlia Lithwick, "How OWS Confuses and Ignores Fox News and the Pundit Class," *Slate Magazine*, Oct. 26, 2011.

69 Katya Komisurak, "Legal Briefing for Activists at the Republican National Convention," *Just Cause Law Collective*, Center for Constitutional Rights, 2007.

WHO NEEDS THE NSA WHEN WE HAVE FACEBOOK?

EVAN TUCKER

ANONYMOUS VS. ANONYMOUS

In the Summer of 2011 the decentralized hacker group Anonymous announced that they wanted to kill Facebook. The YouTube video announcing the attack proclaimed:

> Your medium of communication you all so dearly adore will be destroyed. If you are a willing hacktivist or a guy who just wants to protect the freedom of information then join the cause and kill facebook [*sic*] for the sake of your own privacy. Facebook has been selling information to government agencies and giving clandestine access to information security firms so that they can spy on people from all around the world. Some of these so-called whitehat infosec firms are working for authoritarian governments, such as those of Egypt and Syria. Everything you do on Facebook stays on Facebook regardless of your "privacy" settings, and deleting your account is impossible, even if you "delete" your account, all your personal info stays on Facebook and can be recovered at any time.... Facebook knows more about you than your family.[1]

Complicating matters, other individuals claiming affiliation with Anonymous denounced the video and said that it was a hoax. Things got ugly when this rival faction published information about a person who had allegedly called for the Facebook attack. Of course, the date for the attack came and went and Facebook was not destroyed. But the threat resurfaced again in January of 2012 and the recriminations resumed.

It appears that the most vocal portion, if not the actual majority, of those in Anonymous champion the importance of social media. Yet the call for the destruction of Facebook seems to suggest a crumbling consensus on the value of the medium. Some of the concerns expressed in the Anonymous communiqué have been raised in the wider society, but they seem to be drowning under a flood of fawning press coverage, awestruck over Facebook's latest innovation. But the radical call to action brings to light a dark side of social media that neither innovation nor regulation can erase.

WHAT'S WRONG WITH FACEBOOK?

SOCIAL MEDIA IS unlike any other surveillance technology that has ever existed.[2] Through its innovative organization and display of information, it offers users an unparalleled sense of self-expression and social connection. Its seductively simple platform enables people to share information about themselves and the people they know without a second thought.

Since the collection and organization of large volumes of data is typically the most challenging aspect of a surveillance operation, the advent of social media has been a boon for law enforcement and others with an interest in managing the people they intend to control and/or profit from. Social media has also been a gold mine for advertisers, who pay top dollar for the information that users voluntarily provide. For these reasons, user privacy is not part of the business model. The service is free only because the user is the product.

Since the website Friendster was launched in 2002[3] the use of social media websites has expanded tremendously, with Facebook alone claiming over 800 million users.[4] The influence of social media has been frequently discussed, but rarely critically. So far as I have seen, there has been no comprehensive, public examination of the negative impacts that social media has on our lives, communities, and political movements.[5]

There are four serious problems with social media. These are:

1. Information is not secure. All user-submitted content is controlled by corporations, which freely share it with the government and sell user information to other businesses.

Radio International, Jan. 21, 2011.

51 Anonymous, "Clay Shirky on Twitter and the Social Media Revolution," *The Online Journalism Blog*. Paul Bradshaw, Nov. 7, 2009.

52 Evgeny Morozov, "Smart Dictators Don't Quash the Internet," *The Wall Street Journal*. Feb. 19, 2011.

53 Ibid. On the other hand, prior to an August 2011 protest, Bay Area Rapid Transit (BART) Police shut down cell phone service in its downtown stations to prevent the protesters from coordinating their actions through social media. Michael Cabanatuan, "BART Admits Halting Cell Service to Stop Protests," *SFGate*, Aug. 13, 2011.

54 David Meyerm "Twitter, Facebook and RIM 'look Forward' to Riots Talks," *ZDNet UK*, Aug. 12, 2011.

55 Malcolm Gladwell, "Twitter, Facebook, and Social Activism," *The New Yorker*, Oct. 4, 2010. Evgeny Morovoz points out that those strong ties existed between activists in the Middle East before the recent uprisings: "The collaborations between Tunisian and Egyptian cyber-activists—so widely celebrated in the press—were not virtual, either. In the space of a week in May 2009, I crashed two (independently organised) workshops in Cairo, where bloggers, techies, and activists from both countries were present in person, sharing tips on how to engage in advocacy and circumvent censorship…." He further elaborates: "There were many more events like this—not just in Cairo, but also in Beirut and Dubai. Most of them were never publicised, since the security of many participants was at risk, but they effectively belie the idea that the recent protests were organised by random people doing random things online. Those who believe that these networks were purely virtual and spontaneous are ignorant of the recent history of cyber-activism in the Middle East…". Evgeny Morozov. "Facebook and Twitter Are Just Places Revolutionaries Go," *The Guardian*, Mar. 7, 2011.

56 Steve Sherman, "Why Social Media—Even Twitter and Facebook—Matters," *Left Eye On Books*, Feb. 17, 2011.

57 Morozov, "Smart Dictators Don't Quash the Internet."

58 Wayne Hansen, "How Social Media Is Changing Law Enforcement," *Government Technology*, Dec. 2, 2011.

59 Melody Gutierrez, "Controversial T-shirts Puts Twin Rivers Police Department in the Spotlight Again," *The Sacramento Bee*, Oct. 31, 2011.

60 Bill Lindelof, "Twin Rivers School Police Chief Placed on Administrative Leave," *Sacto 9-1-1, The Sacramento Bee*, Nov. 10, 2011.

61 Vivian Ho, "S.F. Cops Accidentally Leaked Occupy Raid Plans," *San Francisco Chronicle*, Jan. 10, 2011.

62 For more information about computer security visit https://help.riseup.net/en/security and http://www.earthfirstjournal.org/section.php?id=4.

63 Christian Parenti, *The Soft Cage: Surveillance in America : From Slavery to the War on Terror*, (New York: Basic, 2003).

64 Jeffrey H. Reiman, *The Rich Get Richer and the Poor Get Prison*, (Needham Heights: Allyn & Bacon, 2001).

33 Sarah Jacobsson Purewal, "Why Facebook's Facial Recognition Is Creepy," *PC World*. June 8, 2011.

34 Sean Teehan, "Facebook Photos Bring Suspensions," *Boston.com*. May 8, 2011.

35 Harvey Jones and Jose Hiram Soltren. "Facebook: Threats to Privacy," Massachusetts Institute of Technology, Dec. 14, 2005, http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf, (accessed Jan. 16, 2012).

36 Cory Golden, "Students Accuse UCD of Trying to 'infiltrate' Protest Groups," *The Davis Enterprise*, Apr. 13, 2011.

37 Anne Reynolds Myler, "RE: URGENT: October 7th Day of Protest," Message to Griselda Castro and Brett Burns, Apr. 21, 2011. Email. http://www.scribd.com/doc/53581856/part-2-of-3-UC-Davis-Docs-Reveal-Officials-Surveillance-and-Infiltration-Tactics-During-Campus-Fee-Increase-Protests.

38 Army Field Manual 3-24 Appendix B: B15, B17.

39 California Penal Code Section 186.22 (f) "criminal street gang" http://law.onecle.com/california/penal/186.22.html, (accessed Jan. 22, 2012).

40 Kim Strosnider, "Anti-Gang Ordinances After City of Chicago v. Morales: The Intersection of Race, Vagueness Doctrine, and Equal Protection in the Criminal Law," *American Criminal Law Review* 39.1 (2002): 101–46. *Race and Anti-Gang Ordinances*. The University of Dayton School of Law, Winter 2002.

41 Katherine Rosenberg, "Myspace: A Place for Gangs," *Victorville Daily Press*, June 6, 2009. Gang unit head Detective Jeremy Martinez says, "They have since taken down that page. I don't know if they got smart or what, but the individual pages are still active. That's how I'm identifying, or trying to identify the gang members. It's a great tool…. Sometimes you get lucky and it has a good photo of them, or it lists where they live or what school they go to…. A few of them actually put their real names." Nowhere does the detective say that these "37 suspected gang members" are wanted criminals or that their Myspace profiles offer evidence of crimes.

42 Author's interview with one of the targets of the raid, Justin Hand. August, 2008

43 Anonymous Analytics, "Who We Are," *Anonymous Analytics*. July 20, 2012. http://anonanalytics.com/.

44 Nate Anderson, "How One Man Tracked Down Anonymous—And Paid a Heavy Price," *Wired.com*. Feb. 10, 2011.

45 Ibid.

46 Darlene Storm, "Army of Fake Social Media Friends to Promote Propaganda," *Computerworld*, Feb. 22, 2011.

47 Brad Friedman, "Democrats Call for Probe Into Chamber's Shady Plot to Sabotage Progressive Organizations." *AlterNet*, Mar. 1, 2011.

48 Eric Lipton and Charlie Savage, "Hackers Reveal Offers to Spy on Corporate Rivals," *The New York Times*, Feb. 11, 2011.

49 Ashlee Vance and Brad Stone, "Palantir, the War on Terror's Secret Weapon," *Bloomberg Business Week*, Nov. 22, 2011.

50 Marco Werman, "Clay Shirky and the Political Power of Social Media," *The World*, Public

2. The amount of information generated is enormous. Social media's popularity and ease of use have created an ever-expanding database—larger than any in history—allowing the government to prosecute more people and businesses to extract more profit.

3. User profiles are nothing more than dossiers voluntarily created and published by the subject. A self-created dossier can be more revealing than one created by an intelligence agency.

4. Social media automates and simplifies the mapping of interpersonal associations and social networks.

Social media normalizes relentless record-keeping of our lives and tracks us like never before. These sites give governments and businesses access to information that they would never have the time or resources to acquire on their own. It also avoids the scandal associated with the exposure of massive surveillance programs, because the subjects of these dossiers are the same people who produce and disseminate them.

While some users may take self-censoring steps to mitigate the problems, these four aspects are interconnected and inherent to the technology. If you use social media and don't provide much information about yourself, your profile may not be much use to the government, but it probably isn't much use to you, either.

Let's consider the problems in more detail:

1) INFORMATION IS NOT SECURE. ALL USER-SUBMITTED CONTENT IS CONTROLLED BY CORPORATIONS, WHICH FREELY SHARE IT WITH THE GOVERNMENT AND SELL USER INFORMATION TO OTHER BUSINESSES.

In a 2006 article about Myspace, *Newsweek* aptly described it as "a searchable, public scrapbook of images, affiliations and written exchanges" that hands law enforcement data on millions of "potential suspects, witnesses or victims."[6] The privacy implications are astounding, though many people feel that their information is secure because they have chosen a privacy setting that limits access to their profile.

Myspace and all similar websites have so-called "privacy policies." These policies are little more than memos to users hinting at the privacy violations that await them. (And, of course, the terms and conditions are subject to change at any time). In its privacy policy, Myspace indicates that it records user IP addresses for "security purposes." Their privacy policy acknowledges that the company will provide a user's personal information to "comply with the law or legal process" and that they will "access or disclose" it if they think it necessary to "protect the safety and security of Users of the Myspace

Services or members of the public" or for "risk management purposes." The meaning of "risk management" is left unexplained.[7]

Facebook's privacy policy states: "We receive data about you whenever you interact with Facebook.... When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video." Their policy later states, "We receive data from the computer, mobile phone or other device you use to access Facebook. This may include your IP address, location, the type of browser you use, or the pages you visit.... When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services."[8] Keep in mind, however, that Facebook is not just providing *you* a service; many other people would like that information and Facebook's privacy policy makes it clear they will share the data they collect on you if they believe it is necessary:

> We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves and you from violations of our Statements of Rights and Responsibilities; and to prevent death or imminent bodily harm.[9]

So the company's "good faith" is all that stands between the wealth of data they collect about you, and anyone who asks for it.

Since business and law enforcement prefer accurate information, Facebook does its best to verify what you submit. This issue of identity verification hit the headlines in the fall of 2011 when author Salman Rushdie had his Facebook account deactivated after the company demanded proof of identity. Facebook demanded that Rushdie change the name on his account to his birth name, Ahmed Rushdie, despite his being a world-famous author who has published under the name Salman Rushdie for decades.[10]

Pressure from law enforcement has influenced this effort to force people to use their birth names. But it is not the only reason. Linking a person's "authentic identity" to their Facebook page has become an important part of Facebook's business model. According to Somini Sengupta of the *New York*

16 United States Department of Homeland Security, Citizen and Immigration Services, "Social Networking Sites and Their Importance to FDNS," July 20, 2010, https://www.eff.org/files/filenode/social_network/DHS_CustomsImmigration_SocialNetworking.pdf, (accessed Jan. 16, 2012).

17 SMILE Conference, Advertisement, *SMILE-A LAwS Communications Event.* LAwS Communications. http://lawscommunications.com/smile, (accessed Jan. 16, 2012).

18 *U.S. v. Eric McDavid* et al. criminal complaint. Case # 2:06-MJ-0021, Jan. 17, 2006, http://supporteric.org/sacramento_affidavit___crim_complaint.pdf, (accessed Jan. 20, 2012).

19 Ibid.

20 The informant had a Myspace account that she continued to log on to after their arrest, and FBI case agent Nasson Walker had a Myspace account that he used regularly.

21 *U.S. v. Eric McDavid* et al. Idiosyncratic capitalization in the original.

22 Ibid.

23 Documents from the FBI on Eric McDavid obtained by the author through the Freedom of Information Act.

24 Social networking can continue to haunt people even after they leave prison. On September 16, 2010, a year and a half after his release from prison, environmental and animal rights activist Rodney Coronado was sent back on a probation violation. His offense? Accepting a "friend request" from another activist on Facebook. According to the government, by accepting this request Coronado had violated a provision of his probation that prohibited "associating" with any activists, as well as using an "unauthorized" computer. Adam Federman, "The Persecution of Rod Coronado," *Counterpunch,* Sept. 1, 2010.

25 Andy Furillo, "Sacramento Judge Delays Contempt Decision against Facebook," *Sacto 9-1-1, The Sacramento Bee,* Oct. 11, 2011.

26 Randy Borum and Chuck Tilby, "Anarchist Direct Actions: A Challenge for Law Enforcement," *Studies in Conflict & Terrorism* 28.3 (May–June, 2005): 201–23.

27 In Our Towns, "Impersonation Charged," *Courant.com.* Oct. 25, 2006.

28 Tiffany Kaiser, "NYPD Looks to Mine Social Networks for Info on Criminal Activity," *DailyTech,* Aug. 11, 2011.

29 Kimberly Dozier, "AP Exclusive: CIA following Twitter, Facebook," *Yahoo! News.* Associated Press, Nov. 4, 2011.

30 Larry McShane, "Facebook Post Wishing Osama Bin Laden Killed Math Teacher Gets New Hampshire Teen Suspended," *New York Daily News,* May 19, 2011. The school refused to comment on the issue, citing student privacy restrictions. It is ironic that the school would invoke privacy as a way to avoid defending their actions rather than as something that would prevent intrusions into a student's personal life.

31 Tracy Gordon Fox, "Extra Eyes Watch Online," *Hartford Courant,* Oct. 29, 2006.

32 "Nation's Attorneys General Announce Nationwide Agreement With Myspace Regarding Social Networking Safety," *NAAG News.* National Association of Attorneys General, Jan. 14, 2008.

When the renegades of Anonymous called for the death of Facebook they were not the first to recognize the damage that is caused by participating in social media. But they may have been the first to challenge us to engage in collective struggle to resist it. Now we must step us to this challenge, and determine what form that struggle will take.

NOTES

1 Rosie Gray, "Anonymous Wants To Destroy Facebook," *The Village Voice*, Aug. 9, 2011, http://blogs.villagevoice.com/runninscared/2011/08/anonymous_wants.php, (accessed June 25, 2012).

2 For the purposes of this article, I define social media as a system of internet-based, user-generated profiles that emphasize the mapping of connections between people and amassing large amounts of personal information. According to this definition websites such as Facebook, Myspace, Twitter, LiveJournal, and Google+ are social media and websites such as Youtube or Indymedia are not.

3 Christopher Nickson, "The History of Social Networking," *Digital Trends*, Jan. 21, 2009.

4 Lori Andrews, "Facebook Is Using You," *The New York Times*. Feb. 4, 2012.

5 In this article I have chosen to focus primarily on the problems encountered by people using social media in the United States. For this reason my criticisms of social media use and admonitions to avoid it are directed at Americans. I will leave it to people outside of the United States to determine if these criticisms are applicable to their movements and their lives.

6 Andrew Romano, "Walking a New Beat," *Newsweek*. Apr. 23, 2006.

7 Myspace Privacy Policy, http://m.myspace.com/settings/privacy.wap?bfd=offdeck&p=11, (accessed Jan. 15, 2012).

8 Facebook Privacy Policy, http://www.facebook.com/about/privacy/your-info#inforeceived, (accessed Jan. 15, 2012).

9 Facebook Privacy Policy Block Quote, http://www.facebook.com/about/privacy/other, (accessed Jan. 15, 2012).

10 Somini Sengupta, "Rushdie Runs Afoul of Web's Real-Name Police," *The New York Times*. Nov. 14, 2011.

11 Ibid.

12 Michael Liedtke, "FTC: Facebook Misled Users on Privacy," *Telegram.com*, Nov. 30, 2011.

13 Ibid.

14 Romano, "Walking a New Beat."

15 John Lynch and Jenny Ellickson, "Obtaining and Using Evidence From Social Networking Sites," United States Department of Justice, Computer Crime and Intellectual Property Section, Mar. 16, 2010, https://www.eff.org/files/filenode/social_network/20100303_crim_socialnetworking.pdf, (accessed Jan. 16, 2012).

Times, "Forrester Research recently estimated that companies spent $2 billion a year for personal data." Companies like Facebook hope to peddle users' real names as a virtual passport to be used to sign in to over 7 million websites and applications. As Sengupta points out, "it gives Facebook a trail of valuable information about the reading, listening, viewing and buying habits of its users."[11] This information is the product in a multi-billion dollar industry that creates financial incentives for minimizing user privacy and anonymity.

A Federal Trade Commission (FTC) complaint alleges that Facebook has violated users' privacy in a variety of ways including: continuing to display photos that users have deleted, changing privacy settings without permission, and selling users' information to third parties despite claims to the contrary. According to Michael Liedtke of the Associated Press, Facebook is "trying to make money by mining the personal information that it collects to help customize ads and aim messages at people...." Liedtke also points out, "That strategy has been working well as Facebook prepares to sell its stock in an initial public offering that's expected next year." During the period of the privacy violations, Facebook's revenue increased from $777 million to $4.3 billion.[12]

Facebook is not alone. Both Google and Twitter have likewise been the subject of FTC complaints for how they have handled users' information.[13]

2) THE AMOUNT OF INFORMATION GENERATED IS ENORMOUS. SOCIAL MEDIA'S POPULARITY AND EASE OF USE HAVE CREATED AN EVER-EXPANDING DATABASE—LARGER THAN ANY IN HISTORY—ALLOWING THE GOVERNMENT TO PROSECUTE MORE PEOPLE AND BUSINESSES TO EXTRACT MORE PROFIT.

Despite the FTC's action against social media companies, government agencies often rely on these sites to get private information about users. Companies like Myspace are quite comfortable assisting these agencies. In 2006, *Newsweek* reported that "a 20 member, 24/7 law enforcement team fields 350 calls a week from its rolodex of nearly 800 agencies, helping them surf the site." The article goes on to say, "Communication between cops and the two-year-old company has surged this year, with Myspace now contributing to about 150 investigations a month, according to Jason Feffer, its vice president for operations." The same article states that "under Justice Department guidelines, anything posted online is fair game." Myspace ought to be familiar with Justice Department guidelines since they hired former federal prosecutor Hemanshu Nigan to monitor the site.[14]

Social networking sites have become such a rich source of information that law enforcement agencies now prepare trainings on how to use them for investigations. In March 2010, the Electronic Frontier Foundation received documents through the Freedom of Information Act regarding a Justice

Department presentation entitled "Obtaining and Using Evidence from Social Networking Sites." The documents indicate some of the ways the U.S. Department of Justice uses social media: "Reveal personal communications; Establish motives and personal relationships; Provide location information; Prove and disprove alibis; Establish crime or criminal enterprise."

One section title asks, "Why go undercover on Facebook, Myspace, etc"? The text provides the following answers: "Communicate with suspects/targets; Gain access to non-public info; Map social relationships/networks." In a section on witnesses, where the authors ominously proclaim "Knowledge is power," they urge attorneys to "Research all witnesses on social-networking sites" and "Advise your witnesses: Not to discuss cases on social-networking sites; To think carefully about what they post."[15] Ironically, if everyone took their advice, the Justice Department would probably find these sites much less useful.

Also among the documents the Electronic Frontier Foundation received was a 2010 Department of Homeland Security memo entitled "Social networking sites and their importance to FDNS." (FDNS stands for Fraud Detection and National Security.) It states:

> Narcissistic tendencies in many people fuels [*sic*] a need to have a large group of "friends" link to their pages and many of these people accept cyber-friends that they don't even know. This provides an excellent vantage point for FDNS to observe the daily life of beneficiaries and petitioners [*sic*] who are suspected of fraudulent activities.... This social networking gives FDNS an opportunity to reveal fraud by browsing these sites to see if petitioners and beneficiaries are in a valid relationship or are attempting to deceive CIS [Citizenship and Immigration Services] about their relationship. Once a user posts online, they [*sic*] create a public record and timeline of their activities. In essence, using Myspace and other like sites is akin to doing an unannounced cyber "site-visit" on a petitioners and beneficiaries [*sic*].[16]

It's not just the Feds who are catching on to the social media craze, either. All types of law enforcement agencies can register for the Social Media Internet Law Enforcement (SMILE) conference—an annual gathering for investigators looking to "add another weapon to... [their] arsenal." The conference website claims that agencies are using social media in areas such as "community policing, recruitment and retention, investigations, crime prevention, reputation enhancement / management as well as others." In addition to these areas of emphasis the 2012 SMILE conference offers to

that are both real and harmful, the designation of "crime" is not always linked to demonstrable harm: the notion of "crime" requires no such objective criteria. As Reiman points out there are numerous factors in people's lives—such as unsafe working conditions, denial of healthcare, pollution, and high-level fraud—that are rarely considered crimes but cause enormous amounts of harm. "Crime" exists because the state has the power to stand in judgment over people's lives. As the government gains increasing access to those lives through surveillance, their arena of power expands.

Social media creates a relationship of confession and observation between a government and its subjects that facilitates the production of crime. It allows the government and their corporate masters (or minions) unprecedented access to our lives, to our communities, and to our movements. The damage this does outweighs any perceived benefits from increased "communication" or "free" publicity. Joining the site is free, but that is because your relationships, your activities, and your life have become the product. The inclusion of the "knowledge is power" formulation in the Justice Department's training notes should serve as a reminder that the government is empowered, in part, through the collection of information on its subjects. As we accumulate as much knowledge about ourselves as possible, and serve it up to businesses and the state, we give them more power over our lives, voluntarily and necessarily.

We must withdraw our consent from this repressive practice and not accept surveillance as a norm. The Department of Homeland Security mocks users for their narcissism. The Department of Justice says that everything posted online is fair game. The Connecticut Attorney General says that any idea of privacy on social media sites is just an illusion. These are the people who benefit from our use of social media and their proclamations about its dangers offer us compelling reasons to stay away.

While I agree that social movements need media, it is not uncommon for some movements to abstain from activities that have been considered normal social practices (as the use of social media has become). Movements have boycotted elections,[65] or run people for political office who then refuse to serve;[66] many individuals abstain from voting completely.[67] Some activists refuse to talk to corporate media.[68] And of course many activists refuse to talk to law enforcement under any circumstances.[69] These are but a few examples of instances when political groups or social movements refuse to participate in normal social practices that harm their interests. In many of these cases, the social movements argue that everyone should participate in their chosen tactic to deny the state legitimacy and power. That is precisely what I am advocating: that regardless of political or social affiliation, we reject the minor conveniences that participating in this insidious system of surveillance affords us, in order to deprive businesses and the government of some of the power they have over our lives. Remember: they need us more than we need them.

implemented such policies."[61] The SFPD learned their lesson the hard way: In December 2011, participants in Occupy San Francisco learned of an imminent raid on their camp by reading a police officer's Facebook and Twitter posts.

These blunders point to one of the only legitimate uses of social media—intelligence. That is its true function and that is why we must remove ourselves from it. Yet law enforcement and government officials are no less foolish than the rest of us. It appears that they expose, embarrass, and incriminate themselves on social media as much as anyone else does. Since social media is a corporate project with a track record of government cooperation, we are at a distinct disadvantage. Yet as long as they continue to present us with information that can help us fight repression and injustice, we must seize it. The task is to find a way to do this without exposing ourselves in the process.[62]

KNOWLEDGE IS POWER

The use of social media increases the risk of surveillance, repression and incarceration. It is a gold mine for anyone—from cops to school officials to private businesses—looking to collect information. It makes students easier to manage, movements easier to dismantle, and all kinds of people more likely to be harassed or arrested by law enforcement. As Christian Parenti said in his book *The Soft Cage,* "With a little imagination one can see that no matter how mundane, surveillance is also always tied up with questions of power and political struggle."[63]

Yet, the dangers of surveillance are often waved away by people who think that they have nothing to hide. This carefree, and sometimes self-righteous, attitude relies on the assumption that the collection of information is an essentially neutral process, and only has negative consequences for those committing crimes. But it is through the very act of surveillance that crime is produced.

Philosopher Jeffrey Reiman argues that the idea of "crime" is created through agents of the law defining certain acts as crimes and certain people as criminals. Reiman asserts that the concept of crime is an important tool to allow the wealthy and powerful to maintain control over everyone else without really keeping us safe. In his book *The Rich Get Richer and the Poor Get Prison,* Reiman argues that "on the whole, most of the system's practices make more sense if we look at them as ingredients in an attempt to maintain rather than reduce crime."[64]

Surveillance is one of these practices. By dramatically enhancing the government's ability to surveil people, social media users enhance the government's ability to produce crime. While clearly there are acts labeled criminal

educate cops on how to use social media for explicitly political purposes. Their website reads, "This (the fourth) SMILE Conference will also emphasize *the changing role between law enforcement, social activists and traditional media.* Tuesday will offer an entire day of topics covering social activists' interference with investigations, maintaining public order, and mass surveillance in an open source world."[17]

The case of *U.S. v. Eric McDavid* et al. offers us an early example of this "changing relationship between law enforcement, social activists and traditional media." In 2006 McDavid and his codefendants, Zachary Jenson and Lauren Weiner, were arrested and branded as eco-terrorists due to the efforts of an FBI informant called "Anna." The informant traveled to activist gatherings and protests from 2003–2005 trying to gather information and encouraging attendees to break the law. According to FBI agent Nasson Walker, "the information she has provided has been utilized in at least twelve separate anarchist cases."[18]

The FBI's motivation for pursuing McDavid can be summed up by the first line about him in the criminal complaint: "Eric McDavid, age 28, is an anarchist…." The word "anarchist" appears in the fifteen-page complaint no less than twenty-six times.[19]

After the three were arrested, it came out that the government was monitoring the Myspace accounts of Jenson and Weiner. (McDavid did not have one).[20] In the discovery process, the government turned over printed copies of Jenson and Weiner's Myspace pages, including all of their blog posts, comments, and friend listings. The criminal complaint that charged the three with "conspiring to damage or destroy certain property by explosive or fire" referred to Zachary Jenson's Myspace page and quoted from it extensively. The complaint states:

> Jenson, like McDavid, is security conscious and is careful not to disclose information on his website regarding his politically-motivated illegal activity. In one journal entry, Jenson recounts illegal activity he conducted somewhere in the San Francisco Bay Area. A verbatim text of the entry, dated May 21, 2005, reads as follows:
>
> "what happened friday night can't be told here online. it can only be told in person, so everyone back home will have to wait because of security. imagine: music blaring, kids running in the streets, dancing and shouting, adrenaline surging, cops right behind us. we ran fast. and you know what kind of tags were left upon the concrete. yeah, you know."
>
> The FBI JTTF [Joint Terrorism Task Force] has researched the above-described incident and concluded that it took place

> at a protest in downtown Palo Alto, CA. During this incident, dumpsters were moved and overturned in the streets, store windows were broken, and graffiti was sprayed on walls and sidewalks. Photos of the protest obtained through a public source depicts an individual spray-painting the phrase, "pandas are sexy" onto a sidewalk. Jenson's web page contain(s) numerous references to pandas and the "panda house," Jenson's name for his former residence....[21]

Clearly Jenson's concerns about security were warranted, even if his response to them was idiotic.

At Zachary Jenson's bail hearing, his Myspace and LiveJournal accounts were referenced frequently. A straight-faced prosecutor announced that on Jenson's Myspace page he admitted to being a "ninja" and an "assassin," thus proving that he was too dangerous to be released on bail. The prosecutors also used information from Jenson's Myspace account to argue he had no residence and no ties to a particular geographic community and was therefore a "flight risk." No independent corroboration was required for these claims because they were Jenson's own words. Jenson was denied bail.

Weiner was released because she quickly agreed to cooperate with the government and testify against her codefendants. Her family posted the $1.2 million bail.

McDavid, like Jenson—and partially *because of Jenson*—was also denied bail. Though McDavid did not have a Myspace account, Jenson's Myspace page was offered as representative of McDavid's behavior and as a source of insight into his activities. The criminal complaint states: "Jenson's site also contains several journal entries in which he documents his interactions with McDavid. Information from Jenson's journal entries corroborates reporting from the CS [confidential source] regarding McDavid and Jenson's travels."[22] Documents obtained through a FOIA request make it clear that the government was using Jenson's Myspace to track McDavid's whereabouts and obtain information about who his friends might be.[23] Even though McDavid had no Myspace page of his own, Jenson did the damage by putting information about McDavid on his page. McDavid was ultimately sentenced to nearly 20 years in prison.[24]

McGregor Scott, the U.S. Attorney who aggressively pushed for the prosecution of McDavid, went into private practice in 2009 and was retained in 2011 to represent Facebook from his Sacramento office. Ironically, Scott represents Facebook in one of the few reported cases where they are *refusing* to turn over user information. This time it is being requested by defense attorneys to prove juror misconduct.[25]

making the existing social order more efficient. They are not a natural enemy of the status quo."[55]

In response to Gladwell, Steve Sherman argues that media has always been important for social movements and that these movements must adjust to technological change to be successful.[56] But let me be clear: my argument is not against social movements using media or technology. I am arguing that social media, specifically, is unlike any technology that has existed before, and that the collection of corporations that has come to be called "social media" is dangerous and destructive.[57]

As activists, we may want to reach as many people as possible and gain approval for our marginalized causes, but too often we have lost sight of the effects of the tools we use. The fact that people see social media as a tool for social change is more a triumph of marketing than the result of some digital revolution. Social media is a powerful tool for the very institutions that we are at war with, the people that seek to exploit and oppress us. Embracing it has resulted in our willing participation in a process of surveillance that we should be actively resisting.

FROM COUNTERINSURGENCY TO COUNTERINTELLIGENCE

Of course surveillance can be a two-way street. In an article about social media and law enforcement, the website *Government Technology* observed, "Although social media can help enlist public support it can also turn on a dime and do the opposite." Their prime example is from Albuquerque, New Mexico where a "police officer involved in an on-duty shooting brought discredit to himself and his department when reporters discovered that he listed his occupation as 'human waste disposal' on a Facebook profile."[58]

Similarly, in October of 2011, the Twin Rivers Police Department in Sacramento, California came under scrutiny when reporters found pictures on Facebook of t-shirts produced and sold by the police union. Those shirts showed a picture of a small child inside a cage with the caption "U raise 'em, We cage 'em."[59] When the photos went public, it exposed the cops' sadistic attitude toward children and their contempt for people in the community, adding to the tension between the police and the population. Within two weeks Police Chief Christopher Breck was put on paid administrative leave without explanation.[60]

According to the *San Francisco Chronicle*, at a recent conference San Francisco Police Commander Richard Corriea told, "the 100 or so police bosses that it was crucial they adopt strong social media policies to avoid security gaffes. A quick survey showed that almost none of the chiefs had

NYU professor Clay Shirky has emerged as one of social media's major public proponents. In Shirky's view, "the political effect [of social media] is principally in allowing people, who are discontent[ed] with their government, to find each other, to coordinate their feelings and to decide to take action."[50] In the introduction to an interview with Shirky the blog *OnlineJournalism* proclaimed, "social media can do everything from cause revolutions to create whole new political parties when done right."[51]

While it is true that people can connect and organize through social media, its use can come with costs such as constant surveillance, arrest, expulsion, deportation, and incarceration. These costs are often downplayed or ignored while the benefits are overstated.

In this vein, much has been made of the role of social media in the uprisings in the Middle East. Visiting Stanford Scholar Evgeny Morovoz suggests that "Perhaps the outsized revolutionary claims for social media now circulating throughout the west are only a manifestation of western guilt for wasting so much time on social media: after all, if it helps to spread democracy in the Middle East, it can't be all that bad." Morovoz has argued that the successful use of social media in countries like Egypt has been largely because the disintegrating regimes have not been very tech savvy. In his article "Smart Dictators Don't Quash the Internet,"[52] Morovoz notes that countries like Russia and China have used social media as a way to manage dissent, identify opponents, and to cripple the communication system of the opposition. Russia, China, and Vietnam have all set up their own social media systems that are controlled by the government and compete, often quite successfully, with Facebook and Myspace. And countries that have experienced recent uprisings with dissidents using social media have learned their lesson: Syria and Iran do not shut down social media websites, they recognize their value as sources for information about the opposition.[53] Likewise, after riots took place throughout England in August of 2011, British Home Secretary Theresa May began to meet with Facebook, Twitter, and Research In Motion to discuss how they can help the British government in times of unrest.[54]

Social media surveillance is not just for riots and revolutions. The government also uses it for managing its citizens and maintaining stability. The purpose of counterinsurgency is not just to put down revolt, but to make sure it never happens.

Malcolm Gladwell argues that "high-risk activism" is an important element of political movements (ranging from the American Civil Rights Movement to the Italian Red Brigades), and that it is necessary for people to have strong ties to engage in this kind of activism together. Social media, in contrast, promotes *weak* ties. In his *New Yorker* article on the subject, Gladwell states, "It makes it easier for activists to express themselves, and harder for that expression to have any impact. The instruments of social media are well suited to

3] USER PROFILES ARE NOTHING MORE THAN DOSSIERS VOLUNTARILY CREATED AND PUBLISHED BY THE SUBJECT. A SELF-CREATED DOSSIER IS MORE REVEALING THAN ONE CREATED BY AN INTELLIGENCE AGENCY.

When testifying in McDavid's trial, "Anna" stated that her first attempt at infiltrating an activist meeting failed because her appearance did not adequately resemble the people she was trying to deceive. Though she never explained how she finally got it right, it's clear that social media was an important tool for validating her false identity and keeping tabs on the people she met. But the abundant and well-packaged information people have on their profiles has an even more important use for informants.

In their 2005 ethnography of anarchists in *Studies in Conflict and Terrorism*, Eugene police officer Chuck Tilby and University of South Florida psychology professor Randy Borum state that "infiltration is made more difficult by the communal nature of the lifestyle (under constant observation and scrutiny) and the extensive knowledge held by many anarchists, which require [sic] a considerable amount of study and time to acquire."[26]

The success of law enforcement infiltration tactics hinges on believability. If police or informants cannot convincingly impersonate anarchists (or environmentalists, animal rights activists, etc.), then they cannot gain the trust of those people. Without the opportunity to build trust quickly, the ability to manipulate people is severely diminished. Social networking websites could be the ideal text for the necessary study. By offering complete profiles of individuals in social and political groups it gives informants all the information they would need to pose as a member of that group.

Police and prosecutors are unabashed about their regular and widespread reliance on social networking sites. Police can create false profiles for surveillance purposes, but ordinary social media users who do so can be severely punished. (In 2006, a thirteen-year-old girl from Farmington, Connecticut was charged with criminal impersonation because she created a Myspace profile of her principal.[27]) While the sheer number of Myspace profiles may give the impression that there are too many people to effectively monitor, some police agencies are becoming increasingly proficient at dealing with enormous amounts of data. The technology news website *DailyTech* reports that the NYPD plans "to mine social media sites like Facebook, Twitter and Myspace in order to find criminals bragging about a crime they've committed or planning to commit a crime." This is part of a growing trend of tech-savvy law enforcement agencies that have realized they can do more than manually look through these public dossiers. According to *DailyTech*, "New York isn't the only city with positive results from data mining social networks. London's rioters and looters have used Twitter and BlackBerry messages this week to choose targets to burn or loot. Police have been able to use the social networks to find pictures of these criminals."[28]

This data mining is not just used for police work, but for intelligence purposes as well. In a 2012 article about the U.S. government monitoring social media all over the world, Kimberly Dozier of the Associated Press discovered the massive amount of information the CIA is able to collect and process. She reported that, "the CIA is following tweets—up to 5 million a day." Analysts then cross-reference the data with both publicly available information and surreptitiously acquired intelligence to create reports for the White House.[29]

Students from junior high to college are among the millions monitored on social networking. As the *New York Daily News* reports, "A New Hampshire teen discovered that free speech actually comes with a price." In May of 2011, thirteen-year-old Shayne Dell'isola was suspended from Rundlett Middle School in Concord, New Hampshire after posting on her Facebook that she wished Osama Bin Laden had killed her math teacher.[30]

Connecticut Attorney General Richard Blumenthal put it simply: "the illusion of privacy is simply self-delusion on the part of young people." Blumenthal argues that "there is absolutely no reasonable expectation of privacy, which is the test under the law for the requirement of a warrant before the police should use it as evidence."[31]

The more people offer up their personal lives to the internet, the deeper the intrusions become. In January 2008, Myspace made an agreement with fifty Attorneys General, promising to "enhance the ability of law enforcement officials to investigate and prosecute Internet crimes," and to develop "identity verification technology" for the site. A press release from the National Association of Attorneys General also stated there will be scrutiny of "every image and video uploaded to the site."[32]

One of Facebook's methods for scrutinizing every image on their site is using facial recognition software that can automatically identify people in photos. According to Sarah Jacobsson Purewal of *PC World*, "Sure, you can 'opt-out' of the service, but it's a pretty weak consolation. After all, opting out won't keep Facebook from gathering data and recognizing your face—it'll just keep people from tagging you automatically." This technology could potentially make a person identifiable in any picture of them posted to Facebook, including pictures posted without their knowledge or permission. A person does not even need a profile to be identified. Purewal goes on to describe this as "Facebook's way of creating a huge, photo-searchable database of its users. And yes, it's terrifying." Every time a photo is tagged on Facebook, info is added to their massive database of information about the 90 billion photos that they host. And remember: once they have this information, they can give it to anyone they want to.[33]

But it is not only the companies and law enforcement examining young people's profiles. According to the *Boston Globe*, eleven high school athletes were suspended from participating in school sports after a parent found

Those activities are summed up well in a letter written by about a dozen members of Congress calling for investigation in the matter. The letter states:

> The emails indicate that these defense contractors planned to mine social network sites for information on Chamber critics; planned to plant "false documents" and "fake insider personas" that would be used to discredit the groups; and discussed the use of malicious and intrusive software ("malware") to steal private information from the groups and disrupt their internal electronic communications.[47]

One of HBGary's partners in corporate-espionage-for-hire is a Silicon Valley based software company called Palantir. After HBGary's emails were leaked by Anonymous it became clear that Palantir worked with them to prepare a proposal on ways to attack, embarrass, or discredit opponents of the U.S. Chamber of Commerce and Bank of America.[48] Palantir products and services have wide use beyond corporate smear jobs. Palantir's clients in government include agencies such as the NYPD, LAPD, CIA, FBI, and the U.S. Army. The secret of Palantir's success is its ability to take enormous disparate data sets and organize them to create extremely comprehensive pictures of individuals and communities. For example in Afghanistan the U.S. Military uses Palantir to plan counterinsurgency operations. According to a report in *Bloomberg Business Week* the Army can

> type a village's name into the system and a map of the village appears, detailing the locations of all reported shooting skirmishes and IED, or improvised explosive device, incidents. Using the timeline function, the soldiers can see where the most recent attacks originated and plot their takeover of the village accordingly.

Their data aggregation software has domestic applications as well. According to the same report, "the FBI can now instantly compile thorough dossiers on U.S. citizens, tying together surveillance video outside a drugstore with credit-card transactions, cell-phone call records, emails, airplane travel records, and Web search information."[49]

Social media clearly offers a mother lode of information for this handmaiden of repression.

THE REVOLUTION WILL NOT BE FRIENDED

Facebook's defenders make the argument that the technology plays a crucial role in the struggle for freedom worldwide. Since the uprising in Tunisia,

pictures on Facebook of them using alcohol and tobacco. The parent downloaded the pictures and turned them over to the school administration. According to Superintendent Joseph F. Casey, "We are not trying to interfere with what happens outside of schools.... [But] if you're going to represent the school we expect you to uphold that image 24/7." In addition to the athletic suspensions, the school is trying to determine the location of the photos, so that the owners of the house can be prosecuted for allowing underage drinking. If convicted, they could face up to a year in jail and a $2,000 fine.[34]

Universities across the country have indicated that they regularly look at Facebook and will expel students if they see evidence of violations. One student, Cameron Walker, was expelled from Fisher College in Boston for a Facebook post that criticized a campus police officer. Walker later admitted he "was naive about Facebook, because it wasn't affiliated with a university."[35]

Like other government agencies, schools not only monitor social media to control people's behavior, but also to manage dissent. In response to protests against fee hikes, the University of California-Davis created the "Student Activism Team" to spy on students and campus organizations they believed to be involved in the protests. This became public knowledge after a former student received 280 pages of documents through the California Public Records Act detailing some of the University's surveillance activities.[36]

Given the budget crisis that precipitated the protests, it is unlikely that the University has unlimited funds for spying on students. The abundance of up-to-date protest information on Facebook allowed the University to maximize the efficiency and effectiveness of its response. In one email, Associate Director of the Center for Student Involvement Ann Reynolds Myler states, "As we monitor facebook and website announcements to get a better idea of activities for the day, we will finalize the shift schedule for our 16 member resource team."[37] Though schools have rushed to capitalize on the wellspring of intelligence that social media provides, they are just one of many institutions concerned with amassing knowledge to control subject populations.

4] SOCIAL MEDIA AUTOMATES AND SIMPLIFIES THE MAPPING OF INTERPERSONAL ASSOCIATIONS AND SOCIAL NETWORKS.

According to the U.S. Army, one of the key tasks of counterinsurgency is to understand how members of a targeted population interact with each other. The U.S. Military uses a technique called Social Network Analysis to map people's relationships and their connection to any insurgency or political movement. According to Army Field Manual 3-24, "For an insurgency, a social network is not just a description of who is in the insurgent organization; it is a picture of the population, how it is put together and how members interact with one another." The manual goes on to explain the importance of this process by pointing out that Social Network Analysis:

their secrets up in public. But sometimes those secrets are leaked or stolen, as in the case of private security firm HBGary Federal.

Aaron Barr, the CEO of HBGary Federal had a plan to identify members of the hacker group Anonymous and sell the information to the FBI. Anonymous describes itself as a "decentralized network of individuals focused on promoting access to information, free speech, and transparency."[43] They caught the attention of the FBI in 2010 when they shut down the websites of Visa, Paypal and Mastercard in retaliation for cutting off services to the independent news organization Wikileaks.

Barr felt that social media sites were invaluable tools for mapping networks of hackers and uncovering their identities. He even presented a talk at a Justice Department conference about using social media and "specific techniques that can be used to target, collect, and exploit targets with laser focus and with 100 percent success."[44] Despite this brazen boasting he was not successful—in fact, quite the opposite.

Barr created fake Twitter accounts and Facebook profiles to befriend people he believed were "leaders" in Anonymous. He had planned to expose Anonymous members at a February 2011 security conference in San Francisco where he was scheduled to give a talk entitled "Who Needs NSA when we have Social Media?" But he was never able to give that talk. By the time the conference rolled around Aaron Barr and HBGary were in ruins. Anonymous had hacked into HBGary's computer system and made the information they found publicly available online.

Bragging about his efforts in the press unleashed a backlash from Anonymous that cost Barr his job and crushed the company he worked for. Anonymous taunted him with the fact that the information he planned to sell to the FBI was all bogus: "please note that the names in the file belong to innocent random people on facebook, none of which are related to us at all...."[45] Barr was close to erroneously implicating people in hacking activities that they had nothing to do with.

When Anonymous made all Barr's emails public, it became clear that HBGary Federal had been contracted by the U.S. government to create software that would generate fake social media profiles to manipulate public opinion. According to Darlene Storm in *Computerworld*, "It could also be used as surveillance to find public opinion with points of view the powers-that-be didn't like. It could then potentially have their 'fake' people run smear campaigns against those 'real' people." [46]

The leaked emails also indicate that HBGary Federal was hired by the Chamber of Commerce to engage in campaign of sabotage and disruption against their enemies. HBGary's plan included using social media to cause infighting, sway public opinion, and gather information on union activists, their friends, and their families, including their children.

> helps units formalize the informality of insurgent networks by portraying the structure of something not readily observed. Network concepts let commanders highlight the structure of a previously unobserved association by focusing on the preexisting relationships and ties that bind together such groups. By focusing on roles, organizational positions, and prominent or influential actors, commanders may get a sense of how the organization is structured and thus how the group functions, how members are influenced and power exerted, and how resources are exchanged.[38]

In the documents obtained by the Electronic Frontier Foundation, the Justice Department indicates that the ability to "[m]ap social relationships/networks" is one of their primary purposes for using social media. Nowhere is this practice more damaging than in the communities branded with the "gang" or "terrorist" labels.

These labels are defined in part by the beliefs and associations of those being targeted for surveillance, harassment, and prosecution. A crime becomes gang or terrorist activity based on the alleged intentions or loyalties of those accused. When people have this "gang member" or "terrorist" label thrust upon them, activities that would ordinarily be considered legal become illegal, and illegal activities are dealt with much more severely. Relationships, behaviors, and aspects of appearance that are not themselves criminal are used to criminalize communities and support legal interventions.

The California Penal Code defines gangs in the following way:

> any ongoing organization, association, or group of three or more persons, whether formal or informal, having as one of its primary activities the commission of one or more of the criminal acts … having a common name or common identifying sign or symbol, and whose members individually or collectively engage in or have engaged in a pattern of criminal gang activity.[39]

Unfortunately the "common identifying sign" is often race, as the individual accused of membership need not himself have participated in a crime and the "informal" nature of the "gang" leaves little opportunity to disprove membership. Communities targeted for anti-gang efforts often face police occupation and shootings, more frequent arrests, enhanced charges, longer sentences, and further isolation in prison.[40]

According to the *Victorville Daily Press*, officials from the San Bernardino Sheriff's department regularly use Myspace to "track and identify gang members." The Gang Unit of the Sheriff's department began using Myspace after

hearing about the success other law enforcement agencies had with the website. The gang unit uses the profiles of individual Myspace users to get the District Attorney to seek gang enhancements (which increase the length of prison sentences) for people being prosecuted for other crimes. It is unclear if these people would even be considered gang members were it not for their Myspace accounts.[41]

Besides the public goal of prosecuting Internet crimes, law enforcement also uses data from social networking sites to map and analyze political movements and subcultures. Social media makes association more transparent and therefore easier to criminalize. It offers the raw materials for these state-constructed identities.

In 2006, Southern California animal rights activists found out how seemingly innocuous postings on their Myspace pages can have severe consequences. In November of that year, Santa Monica Police, in cooperation with the FBI, raided the homes of eight animal rights activists, trashed their residences, took thousands of dollars worth of property, and ultimately filed no charges. The activists' problems with law enforcement began when they were served with restraining orders to force them to stay away from the property and employees of the beverage company POM Wonderful. POM Wonderful was, at the time, engaged in animal testing and was the subject of regular protests. The restraining order was roughly eighty pages long and included photographs, text, and links from the Myspace accounts of the eight people whose homes were later raided. The information from the Myspace pages was collected by a law firm working for POM Wonderful and included pictures of people passing out information about veganism, attending unrelated protests, and drinking beer. These pictures—along with links to websites such as veganoutreach.org and ecoprisoners.org—were meant to prove that these people were dangerous and supported direct action. While none of the information was linked to any actual crime, all the activists were served with restraining orders, and just over a month later, their houses were raided.[42]

Though much of this chapter focuses on the government's nefarious use of social media, private industry is another culprit. Some businesses engage in surveillance for their own purposes, while others capitalize on the government's outsourcing of intelligence activity. Private security firms are hired to engage in surveillance on behalf of government, so that the dirty work of spying can be done off the books. Little is known about the surveillance practices of businesses in general, and how they use social media in particular. Most of what we know about the government's uses of social media comes from the glimpses gained through the Freedom of Information Act and the cops' propensity to brag about it to the press. The activities of businesses are not covered by the Freedom of Information Act and they are rarely willing to give