11-2013

Social movements using social media in a mined and censored world: examples in the United States and China

Michael Roeder
DePaul University, roedermg@gmail.com

Social Movements Using Social Media in a Mined and Censored World: Examples in the United States and China

A Thesis

Presented in

Partial Fulfillment of the

Requirements for the Degree of

Master of Arts

November, 2013

BY

Michael Roeder

Department of International Studies

College of Liberal Arts and Social Sciences

DePaul University

Chicago, Illinois

ABSTRACT

The purpose of this thesis is to examine data mining and data censorship in the United States and China through the Occupy Wall Street social movement and labor protest activity at the Foxconn, Foshan, and Lock factories. The question posed relates to the level of investment the U.S. and Chinese governments have made in data mining and data censorship to create either a predictable situation with regard to social movement activity, or to impede communication between social movement organizers in the attempt to stop protest. For the U.S. example, I outline the legal history and interpretation of the 4th Amendment as pertaining to data mining policies enacted now to show the legality of governmental actions regarding data surveillance. The evidence of this is in the Occupy Wall Street example, as I use Freedom of Information Act requested documents to show governmental agencies infiltrating and surveilling activity of the OWS movement using data mining. For the Chinese example, I outline the legal history of data censorship as explained through Chinese legal code. Evidence of these practices is shown in communication issues found amongst protestors in Foshan, Lock, and Foxconn factories. I conclude my argument with an alternative to the U.S. and Chinese methods in German rasterfahndung, or data screening. I describe rasterfahndung as a less extreme example of data mining that has evolve over time to exhibit an open dialog for change in mining policies as opposed to blanket, legal mining in the U.S.

CONTENTS

FIGURES

ABBREVIATIONS

OWS	Occupy Wall Street
NSA	National Security Administration
FISA	Foreign Intelligence Surveillance Act
FoIA	Freedom of Information Act
EFF	Electronic Frontier Foundation
ToS	Terms of Service
DHS	Department of Homeland Security
NGO	Non-governmental Organization
GAO	Government Accountability Office
FBI	Federal Bureau of Investigation
ISP	Internet Service Provider
HFS	Human Flesh Search Engine
GDP	Gross Domestic Product
ACFTU	All-China Federation of Trade Unions
DDoS	Distributed Denial of Service
SARFT	State Administration of Radio, Film, and Television

ACKNOWLEDGEMENTS

A special thank you to my family, Michael McIntyre, and Kate for keeping me motivated through my research. Without them, this would not have been possible.

CHAPTER 1: INTRODUCTION

On December 17th, 2010, in Sidi Bouzid, Tunisia, Mohammad Bouazizi began his day like any other, setting up his vegetable stand in the street. Bouazizi had been harassed by police before for not having a license, but the laws in Sidi Bouzid are unclear about whether a merchant needs a permit to sell produce in the street. He was approached by a female police officer who spat in his face, slapped him, and insulted Mohammad's deceased father in front of all the other street vendors. Enraged, Mohammad stormed to the governor's office to speak with him about the treatment he had endured, yet he was denied entry and rejected to speak his case. He threatened to "burn himself" if he was not heard, and after his words fell on deaf ears, he soaked himself in gasoline and lit himself on fire in the middle of mid-day traffic in protest.

Self-immolation has been used in previous protests in the world; however, Mohammad's actions would start not only one of the largest strings of social unrest in the Middle East, but also rapid change of regimes thought impregnable. Within nine months of Mohammad's act, not only Tunisia, but Egypt, Yemen, and Libya witnessed citizen uprisings that rapidly overthrew their governments. In as little as one month (Libya took six months), governments crumbled and leaders were exiled, imprisoned, or killed. As the world watched, many scratched their heads wondering how such results were achieved so quickly. As the events of these revolutions became known through live videos from cell phone cameras, Twitter accounts with millions of responses, and Facebook pages, many became convinced that social media was the vehicle for change in the Middle East.

Writers and journalist worldwide used the term "Twitter rebellion" to describe these revolts. This generally made sense; leaders in Middle Eastern countries were caught off guard by an emerging technology and the people adapted before the governments were able to. Social media usage by citizens in Tunisia and Egypt showed a marked increase during the protest and revolts. The link between social media usage and the success of the protests appeared causal to many commentators, but not all observers were sold on the relevance of Twitter and Facebook.

Kathleen Carley of Carnegie Mellon University carried out the latest analysis with intelligent software she developed to comb though media articles from the archive LexisNexis and her results pose a slightly different hypothesis.[1] Her findings suggest that while Facebook, Twitter, and YouTube certainly played a role in the way the Arab Spring unfolded, their influence was far less critical than many had suggested. Social media was not causal. It told people to go here, to do this, but the reason was social influence, not social networking. Social influencers tend to act across all media, regardless.

Phillip Howard of the University of Washington provides a similar analysis where he argues that each of those revolutions was abetted by some sort of media that is new and not controlled by the state. Howard explains that there is "no doubt that social media helped these movements expand faster, but it would be hasty to conclude that Facebook and Twitter were the main drivers." [2]

---

[1] "Was the Arab Spring really a Facebook revolution?," *NewScientist*, April 13th, 2012 http://www.newscientist.com/article/mg21428596.400-was-the-arab-spring-really-a-facebook-

[2] Philip N. Howard, "Opening Closed Regimes: What was the role of social media during the Arab Spring," *University of Washington Press* (2011): 2.

A popular school of thought amongst social movement leaders is that social media will assist in mass communication through digital channels. While this may or may not be true for the Middle East, a different dialog is present in powerful states such as China and the US. I argue in this thesis that powerful nations such as the US and China are able to use advanced government surveillance as well as tactics of suppression and censorship that limit the effectiveness of social media as the main vehicle of communication to protests and movements. With the vast majority of movements using social media to relay their message across a larger audience, enhanced data mining and censorship techniques have proven to be effective in stopping or slowing communication between social movement participants. The examples I will be using as evidence of this are Occupy Wall Street and labor movements in China.

With the level of investment and innovation in data mining, the U.S. and China have the ability to turn social media against social movements through surveillance and censorship. With analog communication (CTV cameras, following suspects physically), surveillance is extremely difficult and costly, steering away governments reluctant to spend the money and time tracing a person. With data mining, complex algorithms can mine millions of blogs, tweets, and e-mails by the click of a mouse. In essence, the utilization of social media in social movements by well-invested nations creates a disadvantage rather than being an effective tool.

The topic of data mining and privacy has expanded tenfold in the past decade (on pace to expand even more in the next decade). I chose social media as a focal point for examination because of its rising popularity of use, as well as the unique legal framework it functions within. First is the size and level of

expansion social media programs and websites have reached in the past seven years. Here are a few statistics to illustrate my point:

- Twitter currently has 500 million users up from 100 million in the middle of 2010.
- Twitter saw a 252% increase in tweets from 2010 to 2011 from 27 million to 95 million
- Facebook currently has 1 billion users, up from 200 million in 2009, which would make Facebook the third largest country in the world behind China and India
- In 2010 during an average 20 minute period there were 5,870,000 wall posts, 2,716,000 photos uploaded, and 10,208,000 comments posted [3]

The size and expansion of these social media giants is unquestionable, as media websites like Facebook and Twitter are borderless and fully international.

Second, speed of delivery is relevant with respect to organizing large amounts of followers. Dating back to the invention of the transatlantic telegraph cables, rapid communication has evolved to almost instantaneous speeds. Any actor can post a video of a protest with millions of onlookers, receive thousands of comments in a matter of minutes, and suggest action within seconds of the protest occurring. The combination of size, expansion, and speed present a significantly powerful communication tool.

Social movements in the US and China have used tactics similar to the Arab Spring through the Occupy Wall Street movement and the "Jasmine

---

[3] "The Growth of Social Media: An Infographic," Published August 30th, 2011 http://www.searchenginejournal.com/the-growth-of-social-media-an-infographic/32788/.

Movement." These movements have not been as immediately successful as the Arab Spring, which raises the question: how are conditions in the US and China different from conditions in the Middle East? How do the US and China differ from Middle Eastern nations with respect to legal precedent, technology, surveillance, and enforcement? These variables will be analyzed to explore how social media is impacting social movements in China and the U.S.

This study finds that governments of the United States and China both attempt, successfully, to control and monitor social media to create predictable behavior from social movements. In the U.S., this tactic has been successful in quieting the Occupy Wall Street movement, while in China, laborers have resorted to face-to-face conversation on the factory floor to gain success in fighting for wage increases. What distinguishes these two large nations are the tactics used to block, mine, and control data. In the case of the U.S., a unique legal environment has emerged that allows access to citizen data with the Foreign Intelligence Surveillance Act (1978). In 2005, James Risen and Eric Lichtblau published an article in the New York Times claiming the National Security Agency was illegally obtaining citizens' information without the warrant required by this act. Once public, the Electronic Frontier Foundation challenged the government directly, naming the telephony giant ATT as a co-conspirator. The government amended the act in 2008 retroactively, which made ATT not guilty of being an accomplice and the EFF lost its case based on how the term "search" in the 4th amendment was interpreted by the Supreme Court. This opened the doors to data mining of all forms and was the turning point for privacy of user data in social media.

In China the government has admitted they censor and infiltrate citizens conversations. The evidence of this is twofold: the history of data censorship and suppression of major historical events like Tiananmen Square and labor movements, as well as the banning of popular social media websites like Facebook and Twitter, which were replaced by government-approved companies Sina Weibo and Renren. In addition, the government conflicted with Google's privacy practices and replaced Google with an alternative search engine Baidu, which is the most popular search engine in China. The infiltration tactics of the Chinese government are another unique reason China was chosen for this study. The existence of the 50-cent party and the human flesh search engine are phenomena which warrant examination in and of themselves.[4] While other governments may have advanced infiltration tactics, these are publically known and actively debated on amongst citizens.

I will first show how the US invests in data mining as a form of government surveillance through the Department of Homeland Security and National Security Agency. I will begin with a brief synopsis of the legal history of citizens' electronic privacy as well as challenges to the Fourth Amendment in U.S. courts. I will explain how citizens' claims to electronic privacy came into the public eye and where those claims currently stand. I will then outline the various forms of social media in the U.S. and how they are used by citizens as vehicles of communication for social movement activity. I will give details of privacy statements from social media companies' disclaimers and how personal information changes ownership once agreed upon by the user. With the change

[4] The 50-cent party is a program designed by the Chinese government to infiltrate citizens' conversations with pro-Chinese rhetoric through government paid employees. The human flesh search engine was created by the Chinese people as a form of blog to out other Chinese citizens of heinous acts and anti-nationalist behavior.

of ownership, I will begin to show how legal precedents have been used to limit data privacy with regard to social media to show how activities of select government agencies are deemed legal. This, in essence, will illustrate the legal discourse and privacy situation under which US citizens have lived in for the past eleven years.

The Chinese government controls public conversation through suppression and infiltration of communication rather than merely surveillance. I will first explain how the Chinese government suppresses citizens' communication by removing or altering data and by outright ownership of social media outlets. This strategy is illustrated by the Chinese/Google conflict of 2010 and censorship of Baidu, the largest search engine in China. In addition I will give examples of information relating to social movement activity that was either removed or altered by the government. The Chinese government also banned Facebook and Twitter, establishing in their place Sina Weibo and Renren, social network websites approved by and censored by the Chinese government.

The Chinese government infiltrates social media through the "50-cent party" and the "human flesh search engine." The 50-cent party refers to government hiring of 280,000 to 300,000 commentators to infiltrate citizens' conversations, injecting pro-government rhetoric while posing as ordinary citizens. The human flesh search engine is more of an example of the lack of privacy in China on the Internet along side self-regulation. Thousands of volunteer cyber-vigilantes expose personal details of Chinese citizens who post

content that are seen as "evil" or unpatriotic in the attempt to publically humiliate them.[5]

This study includes information from many different types of sources ranging from the U.S. Constitution to newspaper articles. Before I delve into what I used to make my argument, I wish to state a brief disclaimer. Due to the nature of this study as it pertains to government surveillance as well as the emergence of social media in the past seven years, many of the sources used are not traditional academic journals and social media theory. The availability of these types of sources at this time is narrow and difficult to find as social media is a new object of inquiry in scholarly work. My prediction is that many scholarly studies will be done in the next decade to examine social media data, however at this time very few exist. In addition, many of the documents relative to government surveillance are but a glimpse into the future of declassified information as much of the data mining and surveillance is hidden from the public view. While I will present all the data available to argue my point, I am a firm believer that much more will be available in the near future.

It is important to begin with the sources that assisted in setting definitions of the terms used in this thesis. There were various academic writings on definitions of social media and social movements that proved helpful in providing background for the descriptive generalization. In addition, a detailed definition of data mining and censorship will be provided, as these are more technical terms not commonly known. I used *Social Media, Political Change, and*

[5] "China's human flesh search engines" published July 3, 2012 http://freespeechdebate.com/en/discuss/chinas-human-flesh-search-engines/.

Human Rights by Sarah Joseph[6] and *Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance* by Heidi McKee[7] as their definitions were clear and concise.

Newspaper articles contained much of the current information available on the topic of data mining. Notably, the New York Times 2005 article written by James Risen and Eric Lichtblau[8] is one of the first reports of illegal wiretapping by the NSA which triggered the inquiries of fourth amendment violations. Other news articles from the San Francisco Chronicle and Foreign Policy magazine assisted with more investigative journalism into specific incidents pertaining to US and Chinese officials mining citizens.[9][10]

The U.S. Constitution as well as U.S. Code will be used to outline the legal background relating to data mining and government surveillance. I will cite from the Foreign Intelligence Surveillance Act of 1978 as well as its amendment in 2008 to show the evolution of legal code that has had a significant impact on legalizing data mining in the US. In addition I will use other legislation and litigation like the Cyber Security Act of 2012, Katz vs. US, and Hepting vs. ATT to emphasize the conflict that continued after the New York Time article. Lastly as part of the conclusion to the thesis I will incorporate a law review article from

---

[6] Sarah Joseph, "Social Media, Political Change, and Human Rights," *B.C. Int'l & Comp. L. Rev.* 145 (2012), http://lawdigitalcommons.bc.edu/iclr/vol35/iss1/3.

[7] Hedi A. McKee "Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance." *Computers and Composition*. In press.

[8] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.

[9] Rebecca Mackinnon, "The (not to great) Fire of China," *Foreign Policy*, April 17th, 2012, http://www.foreignpolicy.com/articles/2012/04/17/the_not_so_great_firewall_of_china.

[10] Bob Egelko, "Monitoring Occupy within rules, FBI asserts," *San Francisco Chronicle*, September 18.

William and Mary College[11] as background to compare data mining legislation in the U.S. to German legal code to offer an alternative look at data mining in other countries.

[11] Paul M. Schwartz, "Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, The State, and New Technology," 53 Wm. & Mary L. Rev. 351 (2011), http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3405&context=wmlr.

CHAPTER 2: LITERATURE REVIEW

There is much debate in the world of technology as to the worth of data mining in society relating to social movements and protest. Many events have occurred throughout the world that have generated discussion on this topic in the last decade. Most recently the Arab Spring movement in the Middle East, quite possibly the genesis of this argument, has caught the attention of social media advocates and journalists. As mentioned previously, journalists and bloggers around the world were reporting on the actions occurring in the participating nations and, at first, many were making a similar argument. As tweets poured in during the protests in Iran and Egypt, the consensus was that the success of these movements rested on new technology, more specifically the social media giant Twitter. Notable quotes during this era ranged from bloggers like Andrew Sullivan, writing for *The Atlantic* stating …"as the regime shut down other forms of communication, Twitter survived. With some remarkable results…"[12] to statements from former national-security adviser Mark Pfeifle commenting that "without Twitter the people of Iran would not have felt empowered and confident to stand up for freedom and democracy."[13]

While data and opinions were circulating the Internet, some opposing commentary began to gain popularity as well. Notable bloggers and writers like Malcolm Gladwell and Evgeny Morozov entered the scene, determined to show a differing take on the events of the Middle East. Gladwell focused on defining how social protest has been effective in the past, through strong-tie connections as opposed to weak-tie connections via social media. He claims social protest is

---

[12] Andrew Sullivan, "The Revolution will be Twittered," *The Atlantic*, June 13th 2009
[13] Mark Pfeifle, "The Nobel Peace Prize for Twitter?" *CSMonitor.com*, July 6th 2009

about the causes, not the tools, repeatedly in his article *Small Change* published in The New Yorker.[14] As for Morozov, cyber-utopianism is the term he coined, defined as a "naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to acknowledge its downside."[15] Before we delve into the two competing sides of the relevance of social media in social protest, a few pertinent terms, commonly used in this thesis, must be defined.

WHAT IS SOCIAL MEDIA?

Social media is defined as a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that will allow the creation and exchange of User Generated Content. Web 2.0 refers to Internet platforms that allow for interactive participation by users.[16] Social media comes in many forms throughout the Internet based on this definition. The most well known outlets of social media are programs and websites like Facebook, Twitter, and LinkedIn. These programs epitomize Web 2.0, allowing user generated content not only to be viewed, but shared across millions of users worldwide. Facebook alone in its most recent quarterly communication advertised 1.06 billion active users on mobile phones and computers.[17] In addition to social media programs, websites incorporate social media and Web 2.0 practices to allow visitors to communicate openly.

---

[14] Malcolm Gladwell, "Small Change," *New Yorker*, Oct 4 2010 www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

[15] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Foreign Affairs, 2011), 234

[16] Sarah Joseph, "Social Media, Political Change, and Human Rights" (Law Review, Boston College, 2012) Winter2012, Vol. 35 Issue 1, p145-188, 146p.

[17] Donna Tam, "Facebook by the numbers: 1.06 billion monthly active users," *CNet*, January 30, 2013 http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users.

Blogs are another popular form of social media that use Web 2.0 ideas. A blog is defined as a discussion or informational site published on the World Wide Web and consists of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first).[18] Many blogs now are outlets for journalists as there is a lack of formal rules and fact checking that most newspapers and magazine publishers have. While personal blogs are mainly used as diaries for individuals, informational blogs have gained the spotlight as of late and, at times, are considered a reliable news source by some.

While there are many forms of social media not mentioned here, blogs and social media programs will be highlighted in this thesis to emphasize relevant points and important data.

SOCIAL MEDIA ENHANCED

The U.S. government has been a staunch public advocate of internet freedom beyond the borders of this country, using the State Department to carry the message. Clay Shirky, a New York University media professor agrees and, in his article "The Political Power of Social Media" published in *Foreign Affairs*, confirms this with a two-prong approach.[19] Shirky argues that internet freedom helps to advance civil society in the long run, while helping to prevent abuses of power in the short term. Other than describing numerous events in recent history that illustrate his point, Shirky argues that the reason the internet is effective is because it enhances the volume of people communicating, and disrupts the monopoly of communication states are used to.

---

[18] Rebecca Blood, "Weblogs: A History and Perspective," rebeccablood.net, Sept 7, 2000 http://www.rebeccablood.net/essays/weblog_history.html.

[19] Clay Shirky "The Political Power of Social Media," *Foreign Affairs*, Jan/Feb 2011, Vol. 90 Issue 1, p28-41.

The first term that Shirky introduces to argue his point is shared awareness, or the ability of each member of a group to not only understand the situation at hand but also understand that everyone else does too.[20] He goes on to state that social media increases shared awareness by propagating messages through social networks. [21] Essentially, Shirky explains that since the inception of Web 2.0, people are able to openly and quickly communicate with each other, share ideas and practices, organize, and respond like never before. He argues that the Internet is the ultimate tool to enhance communication and that the increase in the number of tools available to communicate will enhance the number of conversation and consequently will increase the number of people communicating. He uses examples from history, stating throughout the Cold War, the Unites States invested in a variety of communication tools, including broadcasting the Voice of America radio station, hosting an American pavilion in Moscow (home of the famous Nixon-Khrushchev "kitchen debate"), and smuggling Xerox machines behind the Iron Curtain to aid the underground press, or samizdat.[22]

Shirky also argues that rampant communication creates what he calls the conservative dilemma. He describes this as a dilemma created by new media that increase public access to speech or assembly, with the spread of such media, whether photocopiers or Web browsers, wherein a state accustomed to having a monopoly on public speech finds itself called to account for anomalies between its view of events and the public's.[23] He goes on to note that while particular

---

[20] Clay Shirky "The Political Power of Social Media," *Foreign Affairs*, Jan/Feb 2011, Vol. 90 Issue 1, p28-41.
[21] *Id.*
[22] *Id*.
[23] *Id*.

programs dissenters use may be simple for states to shut down, broader vehicles of communication make filtering difficult and censorship misguided.

Sarah Kessler, in her article entitled "Why Social Media is Reinventing Activism," echoes similar sentiments, describing social media as the ultimate tool to communicate to the masses in order to achieve more effective social movement activity.[24] Most of Kessler's argument is a response to Malcolm Gladwell's coined term "Slacktivism," (which will be address later in this thesis), as her logic opposes Gladwell's with regard to the power of numbers. She claims that the more people who casually engage with a cause, the more opportunities there are to engage individuals past that first step. Accumulating piles of so-called "slacktivists" isn't necessarily a wasted effort if there are steps they can take to deepen their minimally committed engagement.[25] Kessler also quotes change.org founder Ben Rattray who suggests that it might be more effective to mobilize a hundred people using the web to send letters to a single target than to engage in street protest.[26] Kessler notes that change.org wins a campaign – changes a law, policy, or practice – at least once a week.

While Shirky and Kessler display a form of optimism for social media protest, Rebecca MacKinnon in her article, "The (not-so-great) Firewall of China," suggests that attempts to censor social media are unlikely to succeed.[27] MacKinnon refers to a recent article in Chinese news stating despite Weibo's (Chinese government owned, censored Twitter) best censorship efforts, China's chattering classes have outsmarted the system, using literary allusions, code

---

[24] Sarah Kessler, "Why Social Media is Reinventing Activism," *Mashable* (Oct 9, 2010), mashable.com/2010/10/09/social-media-activism.

[25] *Id*.

[26] *Id*.

[27] *Id*.MacKinnon.

words and innuendo to pass around juicy leaks and tidbits from the foreign media about the alleged murder of British businessman Neil Heywood by associates of Gu Kailai, wife of the former Chongqing Communist Party Secretary Bo Xilai, whose fall from grace has precipitated the biggest leadership crisis in China since the Tiananmen Square crackdown in 1989.[28]

MacKinnon continues, stating China's censorship and propaganda may be complex and multi-layered, but they are obviously not well coordinated. She quotes dissident artist Ai Weiwei who commented that while China's Internet censorship system may be the envy of autocrats worldwide, China's leaders need to understand that in the long run it's not possible for them to control the internet unless they shut it off.[29] MacKinnon finishes her piece with statistics from the China Internet Network Information Centre showing Internet users grew 12.3% in one year in China, inferring that censorship is not a long term solution based on the desires of the Chinese people.

SOCIAL MEDIA DISCOURAGED

The Arab Spring movement received great media attention as its dramatic tale unfolded in front of our eyes on the news. Social media was held on a pedestal as the main communication tool that projected these movements throughout the Middle East, but not all theorists and journalists agree with this assessment, in fact some are downright skeptical of social media's relevance altogether. Malcolm Gladwell, blogger and writer for the *New Yorker*, registered his skepticism in his 2010 piece entitled "Small Change: Why the Revolution Will

---

[28] Rebecca MacKinnon, "The (not-so-great) Firewall of China," *Toronto Star* April 28, 2012.

[29] *Id*.

Not Be Tweeted."[30] Gladwell's main argument is simple: real social change is brought about through high-risk meaningful activism, not weak ties and the low-risk social media activism he titles "Slacktivism."[31]

Gladwell frames his argument by using the 1960s sit-ins that began in North Carolina as an example of a movement with strong group identity and ties. He explains that hundreds of successful social movements, like the sit-ins, occurred before the existence of tools like Twitter and Facebook and were arguably more meaningful to the participants and more successful overall.

He goes on to question the participants as well, knowing that the Twitter data from the Iranian Green movement wasn't primarily from Iranians, but mostly Western onlookers commenting on the events without being there. Gladwell quotes Golnaz Esfandiari, from her article "Twitter Devolution" in *Foreign Affairs*, who stated, simply put, there was not a Twitter Revolution in Iran. Western journalists who couldn't reach – or didn't bother reaching? – people on the ground in Iran simply scrolled through the English-language tweets post with tag #iranelection. Through it all, no one seemed to wonder why people trying to coordinate protests in Iran would be writing in any language other than Farsi.[32]

Gladwell also argues that, in combination with strong ties, movements require strategic hierarchies and structure like that of the Montgomery bus boycott. Loosely tied and leaderless social movements he claims have more

---

[30] Malcolm Gladwell, "Small Change," *New Yorker*, Oct 4 2010 www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.
[31] Malcolm Gladwell, "Small Change," *New Yorker*, Oct 4 2010 www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.
[32] *Id*. via Golnaz Esdandiari, "Twitter Devolution," *Foreign Affairs*, June 7 2010 http://www.foreignpolicy.com/articles/2010/06/07/the_twitter_revolution_that_wasnt.

often than not proven ineffective. He summarizes this by stating that because networks don't have a centralized leadership structure and clear lines of authority, they have real difficulty reaching consensus and setting goals. They are chronically prone to conflict and error.[33] Gladwell does admit that social media allows activists to express themselves in a seamless way, but he contends that it makes it more difficult for that expression to have impact.

While some argue that protest via social media isn't meaningful or effective, Philip Dorling in his article "Media is a Double-Edged Sword" states that while protestors use social media to communicate, so do governments.[34] Dorling notes that traditional forms of communication like word of mouth, graffiti, and posters and placards remain essential in the less developed world. He does issue credit (as does Gladwell) to social media for helping spread dissent amongst a larger audience, but he also notes that with the lack of technology found in most lower-income states usually makes other forms of communication more important.

Dorling continues his argument by noting that governments can and do take advantage of new technology as well. He states that governments control the pipes through which information flows…and while they might not be able to block everything they don't like, with sufficient time and resources they can still exert a great deal of control over what information is available to the public.[35] He notes that the Iranian Green movement slowed to almost a halt because of government tactics, and that even the Tunisian government managed to hack the password of nearly every Facebook user in the country regardless of the

---

[33] *Id*. Gladwell

[34] Philip Dorling, "Media is a double-edged sword," Canberra Times, January 29, 2011.

[35] *Id*.

imminent demise of Tunisian leadership.[36] He claims that China, known for censoring content on the internet from its citizens, has demonstrated great sophistication in using the internet to identify, track and control dissidents while encouraging internet activism acceptable to the regime.[37] The second half of Dorling's article echoes the words of Evgeny Morozov, a Russian specialist on new media, who believes most have underestimated the power of authoritarian regimes to use social media and the internet to maintain order.

In an interview, Dorling quotes Morozov to the effect that authoritarian governments have immensely benefitted from the web by using more sophisticated surveillance. Morozov continues his argument stating that using data posted to social media sites, you can actually start identifying which way social sentiment in a country is going.[38] Dorling finishes his article by making an observation that social media and the Internet may be more of a trap as opposed to a positive tool for those campaigning for human rights and democracy.

Morozov not only has completed interviews on this topic, but also has written a book entitled *The Net Delusion: The Dark Side of Internet Freedom* in which he argues that cyber-utopians (defined previously) are naïve about the workings of governments with strong investments in internet surveillance.[39] In addition to arguing against internet romantics, Morozov critiques internet freedom as a beacon of democracy in authoritarian nations. He states that in their refusal to see the downside of the new digital environment, cyber-utopians end up misunderstanding the role of the internet, refusing to see that it

---

[36] *Id*.

[37] *Id*.

[38] *Id*.

[39] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Foreign Affairs, 2011),

penetrates and reshapes all forms of political life, not just the ones conducive to democratization.[40]

As for authoritarian governments, Morozov claims that journalists and bloggers alike blew the cover of internet protestors. He explains:

> Web 2.0 has moved from the periphery of politics in authoritarian states to its very center—not because it has gained in importance or has acquired new abilities to topple governments, but because both leaders and media in the West grossly overstated its role, alerting the dictators to its future significance. But the significance of the Internet, at least when it comes to fostering new public spaces conducive to democratic norms, will only be felt in the long term—and only if the governments are hapless enough to stay out of the process of shaping these spaces according to their own agendas. There is nothing to celebrate here: Seemingly innocuous digital spaces that may have otherwise been left free of government supervision are now watched with more rigor and intensity than antigovernment gatherings in physical spaces. [41]

Morozov goes on to comment that many authoritarian governments are getting nervous that Facebook and Twitter may, since originating in Silicon Valley, be used in the future by the US government to intervene or spy on foreign communication. He finishes by stating that many foreign governments are realizing how much of their citizens' communication is tied to US infrastructure, and with the most recent discovery from Edward Snowden's comments pertaining to NSA internet activity, coupled with German chancellor Angela Merkel's complaint of US spying practices, this concern can be justified.

Both sides of the debate on social media and its place in social protest have reasonable logic and believable premises, but this paper will side with Morozov and take his argument to apply to the governments of the United States and China, not just authoritarian regimes. As I will illustrate in upcoming

---

[40] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Foreign Affairs, 2011), 235

[41] *Id. p.235*

chapters, many instances of social protest utilizing social media in the U.S. and China have failed due in part to increased surveillance and censorship.

CHAPTER 3: METHODS

This topic will be addressed by way of a twofold comparison of the United States and China. With respect to the U.S., two questions will be posed. First, what is the legal regime that permits data mining and internet surveillance; second, what are the negative consequences for social movements of over-reliance on social media? Specific court cases will be mentioned that started not only legal data mining, but also policies inimical to citizen privacy. Sources will likewise be presented to show how over-utilization of social media had negative repercussions for the Occupy Wall Street social movement.

Chinese government censorship of information will be discussed, as will the monopolization of social media applications in an attempt to curb dissenters and control conversation. The question of whether these tactics have been successful and how they have impacted social movements in China will be addressed through numerous sources related to institutional censorship, self-censorship, and labor protests.

Before delving into these important questions and the research methods involved in answering them, a brief disclaimer on what information is and is not available.

In most masters' theses, a combination of primary and scholarly sources are utilized to create a large array of information with a diverse range of perspective. Due to the nature of this project, that wide array was not easily created. The first issue that arose was the availability of confidential or unpublished data. Records of communication between governmental agencies relating to social movement activity are scarce, primarily because it is

intentionally concealed. While some information has come to light from Freedom of Information Act (FoIA) requests, most of the data that might confirm or disconfirm this theory is unavailable. As for the Chinese example, the main tactic used to filter citizens' communication is censorship, an accurate log of which is not known to exist. While the government has admitted repeatedly that user data is censored, censored data in and of itself cannot be reproduced unless it is republished in a non-censored source.

While pertinent data that would bolster this argument may become available in the future, this thesis will draw on the most recently and relevant data available, much of it from nontraditional sources. The majority of sources used in this thesis consist of online journals, electronic articles, journalistic work, blogs, and a few law reviews. Statistical data from Gallup polls will be presented as well to show trends in participation in social movements and social movements' use of social media. Once additional data is declassified and available, a clearer picture will be drawn on the level of mining and surveillance that occurred during the OWS movement.

SOURCES FOR DATA MINING IN THE U.S.

Three Supreme Court cases established the legal basis for data mining: Katz v. U.S., U.S. v. Miller, and Smith v. Maryland. In the case involving Katz, the Supreme Court found the government violated Katz's Fourth Amendment rights due to the installation of a recording device on the phone booth Katz was using to transmit illegal betting. This case is important because it establishes the

notion of "reasonable expectation of privacy" which proved important in future cases of data mining.[42]

The second case is U.S. v. Miller (1976)[43] in which Miller attempts to conceal bank records for his case in District Court. While lower courts find his records to be protected under the Fourth Amendment, the Supreme Court determined that his records were public as he volunteered the information to the bank. The relevance of this case is that it establishes the notion of third-party ownership, another hot button in data mining legislation, emphasizing the rights related to data owned by a third party.

The last case is Smith v. Maryland (1979)[44] in which Smith attempted to have his phone call records withheld from his robbery conviction. District Courts and the Court of Appeals denied him, and when heard by the Supreme Court they denied him as well claiming that the pen register used to track his call records is not a violation of search and seizure. This case is important because it draws on the doctrines of legitimate expectation of privacy and third party ownership.

These two doctrines form the cornerstone of the legal regime governing the data mining of social media applications and websites. Users of social media programs such as Twitter and Facebook must sign user agreements in which they not only shed their expectation of privacy, but also transfer ownership of their personal information to said third party, thus making the manipulation and search of their data legal.

---

[42] "US Supreme Court Center," http://supreme.justia.com/cases/federal/us/389/347/case.html.
[43] "US Supreme Court Center," http://supreme.justia.com/cases/federal/us/425/435.
[44] "US Supreme Court Center," http://supreme.justia.com/cases/federal/us/442/735/case.html.

The search and manipulation of data on blog sites is more prevalent than data mining on social media sites. Many blogging sites available through the internet have similar privacy statements in which data is transferred to a third party. Many users, as I will show, erroneously believe that their data is safe with blogs. However, even removing government surveillance, commercial data mining companies in the U.S. search blogs even more than social media programs. Due to this false belief in the privacy of their communication, blogs are frequently used to protest the lack of privacy in social media.

OCCUPY WALL STREET EXAMPLE

Since Occupy Wall Street, a worldwide social movement, relied extensively on social media to communicate, I thought it necessary to make this a key example for the U.S. The question posed is whether Occupy Wall Street over-utilized social media leading to the demise of the movement. First I will use sources like occupywallst.org, Facebook, and Twitter that show how Occupy used social media during their campaign, followed by a few sources that show the movement being tracked by the government using data mining and surveillance.

The Occupy Wall Street social movement presents many examples of a movement utilizing social media to communicate with followers. One example is the OWS website which hosts a significant amount of data about the movement. The website has a map of all the chapters, a chat or forum section, a how-to guide for movement participants, registration for an e-mail list, and a

calendar with future events. In addition, OWS has a Facebook page[45] that contains a great deal of information on the priorities of the movement and direction of initiatives.

On the website, Occupy also advertises their Twitter handle, @occupyWallst in which the line of communication is always open. Not only do they have a regular Twitter account, but many sub-accounts for each major city that participates in the movement. I will use communication from some of these accounts to show planning and location of protesters, something the government could mine to prepare responses to such activity. In addition, OWS has an emergency alert account that uses text messaging and Twitter to pass on urgent communication namely @occupyalert.

As for the monitoring of the OWS movement, there is a range of documents available that I will present. One set of documents released pursuant to a Freedom of Information Act request executed by the Partnership for Civil Justice Fund, shows rampant communication from the National Operations Center of the Department of Homeland Security to local law enforcement and other centers within DHS. This transcript outlines key cities and activities of OWS as well as instruction of action for law enforcement based on the events that were occurring at the time.[46]

In addition to this transcript, I discuss the relevance of Twitter and Facebook's transparency reports and how they implicate the U.S. government's

---

[45] "Occupy Wall Street Facebook Site," https://www.facebook.com/OccupyWallSt1?fref=ts.

[46] "Homeland Security Documents Show Massive Nationwide Monitoring of Occupy Movement," *Salem News*, May 4th, 2012.

requests for information from the social media giants.[47] In 2012, there were many requests for information relevant to social movements in the U.S. including OWS.

Lastly, there is an occupy archive entitled www.occupyarchive.org that collects all photos, comments, tweets, posts, and video from the OWS movement. This website was created by Sharon Leon, director of public programs at the Roy Rosenzweig Center for the History of New Media. She gathered graduate students from George Mason University to assist her in mining the movement to create a digital record of the events. While not linked to the federal government specifically, this example shows that people without government resources can retrace the events of the movement and publish them openly to anyone.

SOURCES OF DATA CENSORSHIP IN CHINA

I pose two questions to present data on internet censorship and mining within China. The first question asks what methods are used in China to censor citizens internet communication. This question will be answered twofold, first with institutional censorship, and second with forms of self-censorship. The second question asks how forms of censorship in China have prevented social movements that use or attempt to use social media to communicate. While there is an abundance of data on methods for Chinese institutional censorship available (due to the government's admission), finding social movements that are censored by the government is much more difficult as the data is unavailable if censored completely. As explained earlier, history could possibly answer these

[47] "Twitter Transparency Report," last modified July 2, 2012, http://blog.twitter.com/2012/07/twitter-transparency-report.html.

questions fully, however at this time there is simply not enough definitive information to charge this as fact.

Similar to the U.S., China has a legal basis for internet censorship: the Ordinance for Security Protection of Computer Information Systems, the Temporary Regulation for the Management of Computer Information Network International Connection, and Security Management Procedures in Internet Access. The combination of all three laws promotes widespread censorship, government intervention, and protection of "harmful activities."

The first law is the Ordinance for Security Protection of Computer Information Systems, enacted in 1994. This law gave the Ministry of Public Security jurisdiction over all internet security related issues and gave the ministry rights over actions pertaining to citizen behavior as well as foreign.[48] The second law enacted is the Temporary Regulation for the Management of Computer Information Network International Connection which more specifically mandates that all internet service providers route their traffic through a government owned server before citizens have access. This provision added direct oversight to all activity occurring electronically in the borders of China.[49] The third law is the Security Management Procedures in Internet Accessing, which defines what is considered harmful information and activities. The law lists specific actions, mostly involving harmful activity against the state as well as other citizens.[50]

Forms of institutional censorship addressed in this thesis are the 50-cent party, as well as examples of the removal of data, censorship of news outlets, and

[48] "The Internet in China," created June 8th 2010, http://english.gov.cn/2010-06/08/content_1622956_6.htm.
[49] *Id*.
[50] *Id.*

government monopolized social media programs. To describe the 50-cent party, I use an interview between activist Ai Weiwei and a 26-year old man who used to be a member of the party.[51] The previous worker speaks in anonymity to protect his identity and gives an account of his experience interjecting Chinese propaganda into online conversations with citizens.

Another method the Chinese government uses to censor citizens' data is through government monitored social media programs. Google, Twitter, Facebook, and many other internet applications were formally banned beginning in 2008, and quickly replaced with mirror applications namely Baidu (Google), Sina Weibo (Twitter), and Renren (Facebook). Christopher Hughes's journal article "Google and the Great Firewall"[52] provides a historical and reflective account of the conflict between Google and the Chinese government, eventually leading to Google.com and all Google subprograms being banned. Johan Lagerkvist's journal article "Blogging in China"[53] provides the basics of Chinese social media and how it has impacted the public. In addition, Lagerkvist speaks to self-censorship, political discourse amongst Chinese citizens, and how censorship has changed the way they communicate about government affairs.

While institutional censorship is prevalent, self-censorship is a relevant topic for discussion as well. Two types of self-censorship will be explained throughout this section of the thesis; one being the human flesh search engine, the other is political intimidation. Sources that will be used to illustrate the

---

[51] Ai Weiwei, "Meet the 50-Cent Party," *New Statesman,* October 2012, http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party.

[52] Christopher Hughes, "Google and the Great Firewall," *Survival* 52 (2010): 19-26, accessed on April 9th, 2013, doi:10.1080/00396331003764538.

[53] Johan Lagerkvist, "Blogging in China: Party-state, youth, and social change may provide contesting norms." *Intermedia*, March 2010, Vol 38 Issue 1.

actions of the human flesh search engine are "People Powered Search Engines: Cyber Witch Hunts or Public Service?"[54] from the Beijing Review, "A Study of the Human Flesh Search Engine: Crowd-powered Expansion of Online Knowledge"[55] by Fei-Yue Wang and Daniel Zeng, and "Predicting Political Discussion in a Censored Virtual Environment" by Yi Mou and David Atkin.[56] These sources highlight the history, actions, and results of the HFS and how it has impacted citizens' lives in China. "People Powered Search Engines: Cyber Witch Hunts or Public Service?" is a compilation of articles from news writers around the globe, writing their thoughts on the impact of Chinese citizens taking matters into their own hands and outing government officials on the internet. Wang and Zeng's article, "A Study of the Human Flesh Search Engine: Crowd-powered Expansion of Online Knowledge," is considered the first comprehensive empirical study of the HFS using statistics, graphs, trends, and case studies to describe the functions of this phenomenon. Last is "Predicting Political Discussion in a Censored Virtual Environment" by Mou and Atkin whom use the HFS as an example of how Chinese citizens voice their political opinions. Mou and Atkin provide a detailed account of political intimidation as well, leading to the second form of self-censorship.[57]

The second section of self-censorship is related to political intimidation, stemming from actions of the Chinese government against its citizens. Reporters Without Borders data shows over 70 cyber-dissidents have been imprisoned due

---

[54] "People Powered Search Engines: Cyber Witch Hunts or Public Service?," *Beijing Review Forum*, October 23, 2008.

[55] Fei-Yue Wang and Daniel Zeng, "A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge," *Computer Society Magazine*, August 2010.

[56] Yi Mou, David Atkin, and Hanlong Fu, "Predicting Political Discussion in a Censored Virtual Environment," *Political Communication*, Vol. 28 Iss. 3, 2011, **DOI:**10.1080/10584609.2011.572466.

[57] *Id* Mou and Atkin.

to their behavior against the government, making China the largest in the world for jailing violators.[58] While political intimidation would normally be categorized as an institutional form of censorship, the result of the governments' actions in steering citizens away from dissent equates to citizens censoring themselves. "Blogging in China" by Lagerkvist will be used again to emphasize the level of self-censorship in China and how it impacts citizens' voices. Another article "State Censorship of the Internet" in China by Maris Martinsons gives examples of a few Chinese citizens whom have been detained and are serving in prison for their actions against the state.[59] Nina Hachigian's article in *Foreign Affairs* entitled "China's Cyber-Strategy" admits that the strategy of the government is to promote self-censorship by using specific terms in legislation to dissuade citizens from making certain types of comments, punishable by law.[60] Hachigian describes exact wording from government laws and announcements embedded to promote self-censorship like banning "evil cults," "disturbing public order," and "making comments harmful to the honor of China." Lastly, "Organizational Production of Self-Censorship in the Hong Kong Media" by Francis Lee and Joseph Chan speak to self-censorship by media writers in Hong Kong and how self-censorship is aligned with professionalism.[61] In addition, Lee and Chan detail how news agencies in Hong Kong are owned by businesspeople that have formal political appointments in China, or have financial interests.

The second question posed relating to internet censorship in China is whether attempts to use social media in protest have been effective. To answer

---

[58] "China," Reporters Without Borders, http://en.rsf.org/report-china,57.html.

[59] Maris Martinson, "State Censorship of the Internet," *Communications of the ACM* 48 (4): 67.

[60] Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs*, March/April 2001, 118-133.

[61] Francis L.F. Lee and Joseph Chan, "Organizational Production of Self-Censorship in the Hong Kong Media," *International Journal of Press/Politics*, Vol. 14 Num. 1 (January 2009): 112-133.

this question three labor protests will be examined: the Foshan Honda protest, the Honda Lock protest, and the Foxconn protest. In addition, the question of why labor movements have engaged in protest recently will be answered.

To answer why labor protests have been in the spotlight as of late, a number of references will be used. To draw on the management of labor in China, a description of the responsibilities of the All-China Federation of Trade Unions will be provided through Tim Pringle's journal article "Reflections on Labor in China: From a Moment to a Movement"[62] and "Defending Workers' Rights in China" written by Jerry Harris, Robin Munro, and Michael Zhang.[63] Pringle details not only some of the basic responsibilities of the party, but also notes the contradictory nature of the relationship between a government-run labor union, and employee representation. The driving argument in Harris, Munro, and Zhang's article primarily stands on the unrest caused by the state-run labor union, but also on protest regarding the outlawing of alternative unions to represent workers priorities. In addition, wage increases and working hours are mentioned as a main driver of employee action, and most employee action is described as physical and on-site.

The Honda Foshan and Lock protests will be described primarily through press articles, as scholarly journals are not available. Multiple articles from the *New York Times* will be used to describe the events of these protests as they are the bulk of uncensored reporting. "Chinese Honda Strike a Wake-Up Call for Japan" by Hiroko Tabuchi describes the two events occurring at Honda-owned

---

[62] Tim Pringle, "Reflections on Labor in China: From a Moment to a Movement," *South Atlantic Quarterly,* Volume 112, Number 1 (2013): 191-202, doi: 10.1215/00382876-1891323.

[63] Jerry Harris, Robin Munro, and Michael Zhang, "Defending workers' rights in China: an interview with China Labour Bulletin," Race Class 48 (2007):83, DOI:10.1177/0306396807073861.

manufacturing plants in China.[64] Tabuchi also touches on some of the underlying issues of the protests as being the gap in pay between Japanese workers compared to Chinese, and overall salary as being low compared to company profits. David Barboza and Keith Bradsher's piece, "In China, Labor Movement Enabled by Technology," emphasizes the attempted use of social media by labor groups as unsuccessful due to the government intercepting citizens' conversations.[65] Barboza notes that protestors had to resort to text messaging because the social media application QQ, a popular chat program, was unavailable for effective use. "Chinese Workers Gain Strength In Cyberspace" by Jennifer Cheung writing for Forbes.com[66] shows a slightly higher level of optimism for the use of social media in labor protests referencing QQ as a source for communication, however also notes that many protesting citizens are imprisoned for their actions shortly after the end of an event.

The events at Foxconn will also prove valuable in how citizens use social media in protest. "Riot at Foxconn Factory Underscores Rift in China" by David Barboza and Keith Bradsher detail what occurred at the Foxconn plant to cause a riot and workers to protest.[67] While definitive statements on what caused the riot are not given, Barboza received statements from Foxconn officials pertaining to the interpreted beginning. Jennifer Preston's article "Chinese Social Media

---

[64] Hiroko Tabuchi, "Chinese Honda Strike a Wake-Up Call for Japan," *New York Times*, June 1, 2010, http://www.nytimes.com/2010/06/02/business/global/02honda.html.

[65] David Barboza and Keith Bradsher, "In China, Labor Movement Enabled by Technology," *New York Times*, June 16, 2010, http://www.nytimes.com/2010/06/17/business/global/17strike.html?pagewanted=all.

[66] Jennifer Cheung, "Chinese Workers Gain Strength In Cyberspace," *Forbes.com*, June 1, 2011, http://www.forbes.com/sites/jennifercheung/2011/06/01/chinese-workers-gain-strength-in-cyberspace/.

[67] David Barboza and Keith Bradsher, "Riot at Foxconn Factory Underscores Rift in China," *New York Times*, September 24, 2012, http://www.nytimes.com/2012/09/25/business/global/foxconn-riot-underscores-labor-rift-in-china.html.

Accounts Clash With Official Reports on Riot at Foxconn Factory"[68] shows protestors and outside parties attempting to communicate actions on the ground, while the Chinese government reports differently. Also Preston comments that the government was removing posts to Sina Weibo as they were being posted to stop mass communication. Lastly, Adam Hanft's article published through the Huffington Post, "Foxconn and the Curious Silence of Social Media," draws on the lack of media attention these events generated due to the absence of social media reports as well as attention stirred in Western media.[69] Hanft also notes that the protest was fought through NGO's and "traditional channels" as opposed to new digital technology.

[68] Jennifer Preston, "Chinese Social Media Accounts Clash With Official Reports on Riot at Foxconn Factory," *New York Times*, September 24, 2012, http://thelede.blogs.nytimes.com/2012/09/24/chinese-social-media-accounts-clash-with-official-reports-on-riot-at-foxconn-factory/.

[69] Adam Hanft, "Foxconn and the Curious Silence of Social Media," *Huffington Post*, March 30 2012, http://www.huffingtonpost.com/adam-hanft/apple-foxconn-china_b_1392339.html.

CHAPTER 4: DATA MINING IN THE U.S.

The issues raised by data mining and data surveillance in the US directly tie into the past 45 years of case law on the Fourth Amendment to the Constitution, the "Search and Seizure" clause. Many cases have created an environment in which some data mining and data surveillance are legal. Three court cases and one legal code are the main contributors to the status quo. It is important to state the Fourth Amendment in its entirety first, followed by a description of each case. The Fourth Amendment is as follows:

> 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.[70]

The first court case that contributed to the definition of data mining in the U.S. is Katz v. United States (1967). The case involved a petitioner who was attempting to transmit wagering information across state lines in a telephone booth, illegal at the time per 18 U.S.C. § 1084. The FBI planted a recording device outside the booth to record the petitioner's conversation to generate evidence for a conviction. The petitioner was convicted and the Court of Appeals affirmed. When brought to the Supreme Court, the petitioner's Fourth Amendment rights were found to have been violated by the government. The court gave two reasons for its opinion overturning previous courts, explaining that:

> The government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth, and this constituted a "search and seizure" within the meaning of the Fourth

[70] U.S. Const. amend. IV

> Amendment. The Fourth Amendment governs not only the seizure of tangible items, but extends as well to recording of oral statements. [71]

The court determined that since the petitioner was in a telephone booth at the time of his call, he had a reasonable expectation of privacy and a warrant would have been necessary to carry out the recording legally. The second part of the ruling states that because the Fourth Amendment protects *people*, rather than *places*, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure.[72] This case established an important distinction in defining reasonable expectations of privacy, a topic that will be of the utmost importance in data mining legislation.

The second relevant court case is United States v. Miller (1976). During his pretrial defense, Miller attempted to suppress microfilms of checks, deposit slips, and other records relating to his accounts at two banks. He claimed that the subpoena issued was defective because the records had been seized illegally in violation of the Fourth Amendment. The Court of Appeals reversed previous rulings stating that the bank records were constitutionally protected under the zone of privacy. The Supreme Court confirmed the Court of Appeals ruling, and stated that bank records were business records of the banks and not Miller's private papers. The ruling continued:

> There is no legitimate "expectation of privacy' in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit

---

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

[72] *Id*.

> the obtaining of information revealed to a third party and conveyed by him to government authorities.[73]

The conclusion, essential to this argument, is that the issuance of a subpoena to a third party does not violate a defendant's rights, even if a criminal prosecution is contemplated at the time the subpoena.[74] This case establishes that the transfer of ownership of material to a third party negates reasonable expectation of privacy and, consequently, is not considered a violation of the Fourth Amendment. As will be described, the transfer of ownership is a trending topic in data mining with social media programs.

The last court case is Smith v. Maryland (1979). Smith was convicted of robbery after the police installed a pen register on his phone line to record the numbers he dialed. Smith requested that this information be suppressed due to a violation of his Fourth Amendment rights as the register was installed without a warrant. The District Court and Court of Appeals upheld the pen register information as admissible.

The case then went to the Supreme Court, which deemed the pen register installation constitutional, as it was not considered a "search" under the Fourth Amendment. Again, the court claimed that there was no evidence of a legitimate expectation of privacy as numbers dialed into a telephone must be registered by the phone company as normal operating procedure, and so the numbers were deemed to have been volunteered. In the Court's view, when the petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business,

---

[73] United States v. Miller, 425 U.S. 435 (1976).

[74] *Id.*

Smith assumed the risk that the company would reveal the information.[75] The importance of this case is that certain types of information considered "volunteered" by the court's definition are not protected and can be gathered without a warrant.

Lastly, the Foreign Intelligence Surveillance Act was passed in 1978, amended in 2008, and renewed in 2012 in order to grant government agencies the right to monitor electronic communication from foreign and domestic parties considered a threat to U.S. security. The act requires the government to gain approval for surveillance of foreign entities if it is to be monitored for over one year. Domestic surveillance must be approved within 72 hours of initiation. Attention was drawn to the FISA Act in 2005 when the New York Times published an article showing that the NSA was illegally wiretapping American citizens without a warrant.[76] In response, the government passed the FISA Amendment of 2008, granting retroactive immunity to ATT, the telephony giant that conspired with the NSA to monitor of citizens, as well as allowing the government to engage in surveillance without keeping a record of its activities.[77] The act was renewed in December 2012 and continues to permit the government to electronically monitor acts considered a threat to security.

The privacy statements of popular social media sites echo the established doctrine that the transfer of data to a third party does not fall under the jurisdiction of the Fourth Amendment. Twitter, the popular worldwide micro

---

[75] Smith v. Maryland, 442 U.S. 735 (1979).

[76] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times*, December 16, 2005,
http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.

[77] "FISA Amendment 2008," last modified July 8th, 2008,
http://www.govtrack.us/congress/bills/110/hr6304/text.

blogging site, uses their Terms of Service document to emphasize a user's rights to the service. These provisions must be agreed to in order to use the Twitter service, so all members consent to these terms. Found in this document under the "Your Rights" section, the company explains their "rights to a users data by stating submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display, and distribute such Content in any and all media or distribution methods (now known or later developed)."[78] Essentially this clause grants Twitter the right to do whatever they want with a user's data and to share it with any entity. In addition, since user data is passed through the Twitter service, it then belongs to a third party, making all data non-private and accessible to anyone. Furthermore, under the "Restrictions on Content and Use of the Service" section the Terms of Service state:

> …we also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.[79]

This clause allows the government to request user data from Twitter without cause at any time.

Knowing this, Twitter made the decision in 2012 to publish all requests from the government in a section of their site called the Transparency Report. This report shows graphs, statistics, and metrics on the nature of the requests as

---

[78] "Twitter Terms of Service," last modified June 25th[th], 2012 https://twitter.com/tos.

[79] *Id.*

well as the frequency from each country. More notably, the statistics on U.S. government requests show that from July to December of 2012, the U.S. consisted of 81% of all the requests worldwide at 815 requests in 6 months.[80] Ninety percent of the requests were attributed to search warrants, subpoenas, and court orders.[81]

Less well known is how extensively the government monitors data through social media is via popular blogging sites like Google owned Blogger. Google has a single privacy policy, covering all of its services.[82] The privacy statement is similar to that for a user's Google account. For example,

> many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.[83]

The privacy statement continues to outline what data is collected when using a Google account, including Blogger accounts. Six areas are fair game for collecting data: device information, location information, log information, unique application numbers, local storage, and cookies from browsing. All data can be collected at any time without the user manually opting-in to this access. Only "sensitive personal information," defined by Google as medical facts, racial profile, origin information, political commitments, sexual orientation, and religious affiliation,[84] must be opted into. Lastly, upon the creation of a Blogger account, each setting is defaulted to public, meaning if a user does not want their

---

[80] "U.S. Twitter Transparency Report," last modified January, 2013, https://transparency.twitter.com/information-requests/US.

[81] *Id*.

[82] "Google Privacy Policy," last modified July 27, 2012, http://www.google.com/policies/privacy/?hl=en.

[83] *Id*.

[84] *Id.*

data accessible to everyone they must opt-out by changing their security settings.[85]

OCCUPY WALL STREET EXAMPLE

Started on September 17th, 2011, the Occupy Wall Street Movement is defined (per the OWS website) as a

> leaderless resistance movement with people of many colors, genders and political persuasions. The one thing we all have in common is that We Are The 99% that will no longer tolerate the greed and corruption of the 1%. We are using the revolutionary Arab Spring tactic to achieve our ends and encourage the use of nonviolence to maximize the safety of all participants.[86]

In the beginning the OWS movement had success in occupying Zuccotti Park in New York City as well as at Frank H. Ogawa Plaza in Oakland along with public places in many other cities to call attention to their grievances against the U.S. financial system and the stratification of wealth it creates. The movement was met head on with local law enforcement in conjunction with the Department of Homeland Security in an effort to shut down encampments. Over time, the encampments were dissolved in New York as well as Oakland and the physical presence of the movement appeared over. While OWS still exists, many writers and journalists suggest the movement is fading for a number of reasons ranging from a lack of centralized leadership, to protestors engaging in destruction of property in Oakland, deemed unacceptable according to the mission statement

---

[85] "Control Permissions," last modified February 15th, 2013, http://support.google.com/blogger/bin/answer.py?hl=en&answer=42673.

[86] "Occupy Wall Street," last modified April 14th, 2013, http://occupywallst.org/.

noted previously.[87] While those are potential reasons, there is evidence to suggest that the Department of Homeland Security and local law enforcement surveilled and data-mined OWS communications leading to the movement's premature close.

The legal precedent in the U.S. regarding the change of ownership of online material coupled with privacy policies of popular social media outlets puts the content at risk of surveillance and mining by government organizations. In addition, using any public site conveying information can be accessed by a simple search on the internet, making that content widely accessible.

Occupy Wall Street relies heavily on their website to communicate priorities and advertise other methods of communication to their followers. The main sections of the website are the news feed, livestream, infotent, #howto, forum, chat, and map. The newsfeed is a compilation of stories from protestors and does not contain sensitive information. As for livestream, it contains data on all the OWS movements around the world including live chat rooms for participants to discuss local topics. In addition, each section has a live video available to watch.[88] Infotent is a section of the website that informs web users about the priorities of the movement and specifies areas of the U.S. financial system that it is combatting.[89] #Howto is a full guide on how to engage a movement from camping and occupying, to legal and policing issues. This

---

[87] "Occupy Wall Street: The Bloom is Fading," November 7th, 2011, http://www.economist.com/blogs/democracyinamerica/2011/11/occupy-wall-street.
Thai Jones, "As Occupy Wall Street Fades, Powerful Ideas May Live On," *Bloomberg.com*, September 21st, 2012.
"Occupy Oakland: 400 arrested after violent protest," NBCNews.com, January 30th, 2012, http://usnews.nbcnews.com/_news/2012/01/30/10268080-occupy-oakland-400-arrested-after-violent-protest.

[88] "Occupy Streams," http://occupystreams.org/.

[89] "Occupy Infotent," http://occupywallst.org/infotent.

section would be particularly revealing for a data mining program.[90] Forum is also a relatively telling section of the website, as protestors, potentials, or non-followers can read what is going on in each city engaging in the protest. Users can respond with the proper form header to create new posts as they occur in any given city.[91] Chat is a live chat room for anyone who wants to engage or spectate. This could be data-rich if a particular event was taking place.[92] Lastly is the section called map, which shows a map of the world with clickable areas engaging in the Occupy movement.[93]

There is additional public information on the OWS website that is sensitive as well, including an info line with an active phone number, two e-mail addresses for contacting the site administrator directly, the OWS Twitter handle to contact the movement via social media, an Occupy emergency text system in case of an incident, registration for the Occupy mailing list, a link to the OWS Facebook page, and lastly a link to a website that houses all the assembly information for meetings of members of the movement.[94] All these resources, while valuable to the movement, are 100% accessible without intricate technology or masking agents.

All of the information listed above is accessible through common web browsing, but much more information was transmitted via social media and news broadcasts that are not included on the website. A staff of 16 students and faculty from George Mason University created a website titled "Occupy Archive" to track all the data created and transmitted during the movement. The

---

[90] "#Howto Occupy," http://howtooccupy.org/.
[91] "Occupy Forum," http://occupywallst.org/forum/.
[92] "Occupy Chat," http://occupywallst.org/chat/.
[93] "Occupy Map," http://occupywallst.org/attendees/.
[94] "#Occupy Wall Street NYC General Assembly," http://www.nycga.net/events/.

goal of the team was to create a database of information for the Roy Rosenzweig Center for History and New Media, similar to other event databases for September 11th and U.S. hurricane activity.[95] Other than open web searches, the team also used a commercial application called Zotero to rapidly sort through and archive data. The staff archived images, documents, audio, video, and social media tags without the use of sophisticated data mining software. This displays the ease with which a student group mined much of the data available about OWS.

While basic data mining with commercial software appears relatively simple, government mining is far more complex and has become much more common. An article written in the Washington Post in 2006 (pre-OWS) outlines the money spent and companies sought after for such services. Arshad Mohammed and Sara Kehaulani Goo write that

> As federal agencies delve into the vast commercial market for consumer information, such as buying habits and financial records, they are tapping into data that would be difficult for the government to accumulate but that has become a booming business for private companies.
>
> Industry executives, analysts and watchdog groups say the federal government has significantly increased what it spends to buy personal data from the private sector, along with the software to make sense of it, since the Sept. 11, 2001, attacks. They expect the sums to keep rising far into the future.[96]

They continue to describe the change in usage

> It is difficult to pinpoint the number of such contracts because many of them are classified, experts said. At the federal level, 52 government agencies had launched, or planned to begin, at least 199 data-mining projects as far back as 2004, according to a Government Accountability Office study. Most of the programs are used to improve services, such as detecting Medicare fraud and improving customer

---

[95] "Occupy Archive," http://occupyarchive.org/about.

[96] Arshad Mohammed and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining," *The Washington Post*, June 15th, 2006, www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html.

> relations. But a growing number of agencies are exploring the technology to analyze intelligence and assist in the hunt for terrorists.
>
> Another GAO report released in April found that of $30 million spent by four government agencies last year on services from data-crunching companies, 91 percent was for law enforcement or counterterrorism.[97]

Much has changed since 2006 including government spending. The government spent $64.7 billion in 2008 to $82.4 billion four years later in 2012 toward data mining and IT solutions.[98]

While information pertaining to government mining of the Occupy Wall Street movement is scarce, many inferences can be drawn based on what is available. The main documents providing direct data on government surveillance of the OWS movement are a series of unclassified FBI and Department of Homeland Security reports with specifics on movement activity and transmissions between departments. These documents were released pursuant to a Freedom of Information Act request by the Partnership for Civil Justice Fund and provide informative data on the actions of law enforcement and intelligence agencies.[99] The documents are heavily censored, but they do provide data that explains the tactics used by law enforcement to stop the OWS movement, referred to as a terrorist/anarchist movement multiple times in the filing.

---

[97] *Id.*

[98] FCW Staff, "Data Mining: Government spending by the numbers," The Business of Federal Technology, February 12, 2010, http://fcw.com/Articles/2010/02/08/DATA-MINING-egov-satisfaction-IT-spending.aspx.
Elizabeth Montalbano, "Mobile will be government IT's top governance issue, and overall government IT spending will hit $82.4 billion, IDC predicts," Informationweek.com, December 9th, 2011, http://www.informationweek.com/government/cloud-saas/10-government-it-predictions-for-2012-id/232300268.

[99] "FBI Documents Reveal Secret Nationwide Occupy Monitoring," last modified December 22nd, 2012, http://www.justiceonline.org/commentary/fbi-files-ows.html.

The first report to mention the Occupy Wall Street movement is from the FBI branch in New York, dated August 19th, 2011, about one month before the beginning of the movement. The document reports that an FBI agent met with representatives of the NYSE to warn them about a social movement that may target them. The report states that

> …it was discussed that the planned Anarchist protest titled "Occupy Wall Street", scheduled for September 17th, 2011 (could possibly target them.) The protest appears on Anarchist websites and social network pages on the internet. Numerous incidents have occurred in the past which show attempts by Anarchists to disrupt, influence, and or shut down normal business operations of financial districts.[100]

It is noted that the FBI knew about Zuccotti Park over a month before it was occupied by mining data available on the internet relating to OWS. In addition to the NYSE, the report states that Federal Hall and the Museum of American Finance could be targets.

Two days before the Occupy Wall Street movement in Zuccotti Park, another FBI field report from Indianapolis was written warning of "planned nationwide activity." The report groups the OWS movement with another social movement, U.S. Day of Rage, designed to encourage fair voting and representation. The filing echoes topics from the New York report, but elaborates on specifics for September 17th, stating

> In July 2011, Adbusters, a self-identified American revolutionary anarchist group advocated a "take over" of Wall Street in New York on 17 September 2011. The group 'Occupy Wall Street' (http://occupywallstreet.org) is an online social networking offshoot of the declaration by Adbusters. 'Occupy Wall Street' is calling for "20,000 people to flood into Manhattan, set up tents, kitchens, and barricades to occupy Wall Street for a few months."…In their July 2011 declaration, Adbusters initially intended for the event to occur in New York City only; however, as the movement escalated in popularity over the summer

[100] Federal Bureau of Investigation New York, *Field Report New York*, report for 8/22/2011.

> months, unorganized direct action demonstrations are being planned for locations throughout the United States on 17 September 2011. Like 'US Day of Rage,' the group 'Occupy Wall Street' does not openly condone violence or illegal activities; however, their website offers information on "dealing with first responders, chaotic protesting" and suggested that protestors bring "billy clubs and taser guns."[101]

The filing contains basic information about the location and date of the event, two days after the report was written. At the end of the report, it is noted that the OWS movement website offers information on dealing with first responders and chaotic protesting, which has been confirmed upon review of the website. As for the second statement referring to billy clubs and taser guns, that information was found solely in the FBI documents, and in no other source.[102]

New York and Indianapolis FBI reports mixed information available on Occupy's website, with other information apparently not from elsewhere. The Anchorage FBI field report from 3 November 2011 claims there was discussion on the internet regarding the Occupy Wall Street movement about when it is okay to shoot a police officer.[103] In this instance, the OWS website is not referenced as it was in previous reports; instead the data is labeled as "discussion on the internet" about a violent act by protestors. Also contained in the report is a description of how the FBI obtained information about the OWS movement by sending a port Facility Security Officer along with a police officer to infiltrate an OWS meeting. It is not specified how the officials knew when and where the meeting was to take place, but it is plausible that the OWS website contained this data.

---

[101] Federal Bureau of Investigation Indianapolis, *Situational Information Report*, report from 9/15/2011.

[102] The presence of text confirming protestors bring billy clubs and taser guns to a protest would contradict the mission statement of the movement. I was not able to verify this data in other online sources upon researching it. The report does contain a footnote as to the location of the data quoted, however all footnotes and citation have been censored so the root source is inaccessible.

[103] Federal Bureau of Investigation Anchorage, *Field Report Anchorage*, report from 11/3/2011.

An FoIA request report from Anchorage FBI, written on 28 November 2011 stated intelligence was gathered relating to the OWS movement on the port. In this instance, law enforcement used an e-mail claiming action to another undisclosed person, a LinkedIn profile page, and a Facebook printout to gather information on what was to be expected on 12 December 2011. While the source of the e-mail is not noted, report contains the message in its entirety. The report cites an unnamed person who claims he came across this information while perusing various internet sites.[104]

A Jacksonville Florida FBI agent filed a field report relating to electronic communication received from a censored source. An unnamed source claimed to find an e-mail on the social media site UNET, known for private and public level communication as well as stern privacy policies.[105] The information in this e-mail included meeting times and locations of OWS organizers. The informant recommended to the Counterterrorism Program Coordinator that a tripwire system be set up with the Occupy event coordinators regarding their observance of actions or comments indicating violent tendencies by attendees.[106] Tripwires, a form of automated purchase tracking triggered by multiple purchases of suspicious material, have recently been used by the FBI to track down potential terrorist plots.[107] The Department of Homeland Security or FBI set keywords for purchases, like fertilizer used in bombs, and they utilize data mining to track abnormal buying habits as precursors to terrorist activity or acts of violence. In

---

[104] Federal Bureau of Investigation Anchorage, *Field Report Anchorage*, report from 28 November 2011.

[105] "Unet: Social Network," http://www.unet.net/.

[106] Federal Bureau of Investigation Jacksonville, *Field Report Jacksonville*, report from 19 October 2011.

[107] Devlin Barrett, "'Tripwires' Can Spot Would-Be Bombers," The Washington Post April 15, 2013, http://online.wsj.com/article/SB10001424127887324345804578425483373542340.html.

the FBI filings, the Occupy Wall Street movement is repeatedly characterized as an "anarchist, terrorist movement."

An FBI situational information report from Richmond, Virginia recorded a linkage between Occupy Wall Street and the hacktivist group 'Anonymous,' commenting that the group released a video pledging support for the OWS protests and encouraging members to participate. It goes on to state that in the past Anonymous planned cyber intrusion activities or distributed denial of service (DDoS) attacks to coincide with other physical protests. This could indicate an intention to conduct cyber attacks in conjunction with the various Occupy Wall Street protests, including the Occupy Richmond protest. According to open source reporting, Anonymous planned to release a new DDoS tool to the public called RefRef in September 2011.[108] This is another instance in an FBI report in which the source of information is not available, this time with no footnote to substantiate the source's claim. The source of this information in the report is referred to as 'open source reporting.'

The Partnership for Civil Justice Fund made another FoIA request for material more specific to Department of Homeland Security communications with law enforcement as a branch of intelligence. These documents show not only intense government monitoring and coordination in response to the Occupy Movement, but reveal a glimpse into the interior of a vast, tentacled, national intelligence and domestic spying network that the U.S. government operates against its own people.[109] The DHS describes the National Operations Center as,

---

[108] Federal Bureau of Investigation Richmond, *Situational Information Report*, report from 13 October 2011.

[109] "Homeland Security Documents Show Massive Nationwide Monitoring of Occupy Movement – This set of released materials reveals intense involvement by the DHS National Operations Center (NOC) in these activities," *Salem-News*, May 4th 2012.

"the primary national-level hub for domestic situational awareness, common operational picture, information fusion, information sharing, communications, and coordination pertaining to the prevention of terrorist attacks and domestic incident management."[110]

The first example in these unclassified documents is a DHS NOC Fusion Desk report in which a law enforcement official requested assistance in identifying an OWS protestors to make an arrest. The DHS responded with identity and contact information of the group protesting against Bank of America. In the document, it is noted that the NOC used LexisNexis Accurint software to determine the identities of the protestors.[111] According to the user manual of this software, "data mining techniques are used to pull comprehensive data on a citizen using a wide array of sources (unnamed)."[112]

The second example within the documents is a record of a physical meeting between members of the Occupy Wall Street divisions from Toronto, Niagara, Buffalo, and Philadelphia. The report states that there was a planned meeting between thirty representatives on the Rainbow Bridge in Niagara Falls where the members where to discuss how to "bridge the divide" between their respective movements.[113] The document notes the exact coordinates of where the members were standing during the meeting and states that law enforcement was present to observe.[114] How the DHS knew of the location of this meeting, the

---

[110] *Id*.

[111] Department of Homeland Security, *FOIA Transmissions*, report 5 November 2011.

[112] "LexisNexis Accurint Government Sample Reports," https://learn.lexisnexis.com/lexisnexis/user_training.aspx?solution=%23gsr.

[113] The words "bridge the divide" were in quotations meaning that direct communication of this meeting was known ahead of time and signifies exact labeling of the event by probable members of OWS.

[114] Department of Homeland Security U.S. Customers and Border Protection, *Significant Incident Report*, reported on January 1, 2012.

members, the purpose of the meeting, and what group they belong to was blacked-out from the document.

Overall the three documents were very telling of specific operations taken to disrupt the Occupy Wall Street movement. The report is 335 pages long with a vast array of communication pertaining to intelligence gathering against the OWS movement as well as operational steps taken to prevent particular actions. While direct mention of digital tools is not used except for the LexisNexis example, many of the sources of information are redacted to conceal their location so that without proper clearance, the source is obscured.

Since OWS, a significant example of government data mining has been discovered through outcast government contracted, Booz Allen Hamilton employee, Edward Snowden. Snowden, now in exile to avoid U.S. prosecution, exposed the activities of his then employer, the National Security Administration. Laura Poitras, a film maker and producer, and Glenn Greenwald, a columnist at the Guardian newspaper, interviewed Snowden when in Hong Kong after he released confidential information on the NSA's data mining applications and activity. Snowden stated:

> The NSA doesn't limit itself to foreign intelligence; it collects all communication that transits the United States. …One of the programs used was Boundless Informant, which was used as a global auditing system for the NSA to intercept and collect data. The program tracked how much we were collecting, where we were collecting, and by which authority and so forth. …The NSA lied about the existence of this tool to congress in response to previous inquiries about their surveillance activities. Beyond that we have PRISM, which demonstrated how the US government co-opts US corporate power to its own ends. Companies like Google, Facebook, Apple, Microsoft-they all get together with the NSA and provide the NSA direct access to the back-ends of all of the systems you use to communicate- to store data, to put things in the cloud, even to send birthday wishes to keep a record of your life. And they give NSA

> direct access that they don't need to oversee so they can't be held liable for it.[115]

Snowden's account not only affirms the potential for government surveillance on OWS, but is a much deeper and widespread surveillance of American and international communication in all facets. The NSA was put under pressure by U.S. allies after a confidential document was released stating the NSA was monitoring German Chancellor Angela Merkel's cell phone, along with 34 other nations.[116]

This chapter has established three key indicators of U.S. internet surveillance. The first is the legal history creating the current conditions for data mining, beginning with the Fourth Amendment to the Constitution. From there, three Supreme Court cases were detailed along with a description of the FISA Act of 1978 which justified third-party ownership of data along with recent activity by the federal government. The second is a description of two branches of social media along with their privacy policies establishing the transfer of ownership along with illustrating the lack of privacy on social media programs like Blogger and Twitter. In this description, the transparency report issued by Twitter revealed the government's requests of citizen's data.

The third is the Occupy Wall Street movement, along with a full description of all communication avenues that the movement utilizes. A synopsis of the website, along with social media implications, the location of pertinent data, and a description of OccupyArchive was given to show the ease

---

[115] Laura Poitras and Glenn Greenwald, "The US Government Will Say I Aided Our Enemies," *The Guardian*, July 8, 2013, http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.

[116] Laura Smith-Spark and Per Nyberg, "Germany to send intelligence officials to Washington amid spying uproar," *CNN*, October 26, 2013, http://www.cnn.com/2013/10/26/world/europe/germany-us-nsa-spying/index.html?hpt=wo_c1.

with which important data is found on relevant dates, locations, and times of events. This information, partnered with the FoIA requests by the Partnership for Civil Justice Fund, provided evidence linking government surveillance to the movement in many forms. These documents, mostly field reports from the Federal Bureau of Investigation as well as the Department of Homeland Security, show plentiful communication regarding protestors' actions in specific cities, as well as precise knowledge of movement activities before they occurred. The data, while imperfect, illustrates many links between government surveillance and the Occupy Wall Street movement showing that most activities engaged in by the movement were not only under surveillance, but prepared for and infiltrated multiple times. Consequently, in the past year, activity from the OWS movement has declined and mass organizations of members have faded since the movement's inception.

CHAPTER 5: DATA CENSORSHIP IN CHINA

While data mining is a popular method of surveillance in the United States, data censorship is prevalent in China. Data censorship is categorized under two umbrellas: institutional censorship and self-censorship. Each form is unique, yet both have similar outcomes. In this chapter tactics of institutional and self-censorship on the Chinese labor movement will be examined.

China enacted censorship of citizens' online activity by way of three laws. The first is the Ordinance for Security Protection of Computer Information Systems, established in 1994. This act placed all activity online under the jurisdiction of the Ministry of Public Security,[117] the same ministry which has full policing power of all activities within China and investigates law violations on numerous fronts.

Second is the Temporary Regulation for the Management of Computer Information Network International Connection which routes internet activity through a filtering and censoring government firewall. ISPs may deliver services to Chinese citizens, but the Ministry of Public Security must approve content through the firewall. This is the principle means of internet censorship.[118]

Third is the Security Management Procedures in Internet Accessing policy, enacted in 1997, prohibiting "harmful" activities on the web. Articles five and six state:

> inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations; inciting to

---

[117] "The Internet in China," created June 8th 2010, http://english.gov.cn/2010-06/08/content_1622956_6.htm.

[118] Lehman, Lee, Xu, "The Temporary Regulation for the Management of Computer Information Network International Connection," http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html.

> overthrow the government or the socialist system; inciting division of the country, harming national unification; inciting hatred or discrimination among nationalities or harming the unity of the nationalities; making falsehoods or distorting the truth, spreading rumors, destroying the order of society; promoting feudal superstitions, sexually suggestive material, gambling, violence, murder; terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people; injuring the reputation of state organs; other activities against the Constitution, laws or administrative regulations.[119]

Article six states that no individual may use computer networks or network resources without getting proper prior approval, without prior permission change network functions or to add or delete information, without prior permission add to, delete, or alter materials stored, processed or being transmitted through the network, or deliberately create or transmit viruses. Other activities which harm the network are also prohibited. [120] In a nutshell, any act that is considered against social order, or governmental priority, is prohibited based on these laws.

Another form of institutional censorship in China is the '50-Cent Party,' a group of writers paid to infiltrate public opinion online to sway Chinese citizens towards the ideals of the government. They are called the '50-Cent Party' because it is rumored they make 50 cents for every post. Ai Weiwei, the famed artist and social critic, interviews an anonymous member of the"50-Cent Party:"

> **Ai Weiwei Question** – what do you call the work you do now?
> **Answer** – It doesn't matter what you call it: online commentator, public opinion guide, or even "the 50-Cent Party" that everyone's heard of.
>
> **Q** – When and from where will you receive directives from work?
> **A** - Almost every morning at 9am I receive an email from my superiors – the internet publicity office of the local government – telling me about the news we're to comment on for the day.

---

[119] *Id.*

[120] *Id*.

Sometimes it specifies the website to comment on, but most of the time it's not limited to certain websites: you just find relevant news and comment on it.

Q - Can you describe your work in detail?
A - The process has three steps – receive task, search for topic, post comments to guide public opinion. Receiving a task mainly involves ensuring you open your email box every day. Usually after an event has happened, or even before the news has come out, we'll receive an email telling us what the event is, then instructions on which direction to guide the netizens' thoughts, to blur their focus, or to fan their enthusiasm for certain ideas. After we've found the relevant articles or news on a website, according to the overall direction given by our superiors we start to write articles, post or reply to comments. This requires a lot of skill. You can't write in a very official manner, you must conceal your identity, write articles in many different styles, sometimes even have a dialogue with yourself, argue, debate. In sum, you want to create illusions to attract the attention and comments of netizens. In a forum, there are three roles for you to play: the leader, the follower, the onlooker or unsuspecting member of the public. The leader is the relatively authoritative speaker, who usually appears after a controversy and speaks with powerful evidence. The public usually finds such users very convincing. There are two opposing groups of followers. The role they play is to continuously debate, argue, or even swear on the forum. This will attract attention from observers. At the end of the argument, the leader appears, brings out some powerful evidence, makes public opinion align with him and the objective is achieved. The third type is the onlookers, the netizens. They are our true target "clients". We influence the third group mainly through role-playing between the other two kinds of identity. You could say we're like directors, influencing the audience through our own writing, directing and acting. Sometimes I feel like I have a split personality.

Q - Can you reveal the content of a "task" email?
A - For example, "Don't spread rumours, don't believe in rumours", or "Influence public understanding of X event", "Promote the correct direction of public opinion on XXXX", "Explain and clarify XX event; avoid the appearance of untrue or illegal remarks", "For the detrimental social effect created by the recent XX event, focus on guiding the thoughts of netizens in the correct direction of XXXX".

Q - Can you tell us a specific, typical process of "guiding public opinion"?
A - For example, each time the oil price is about to go up, we'll receive a notification to "stabilise the emotions of netizens and divert public attention". The next day, when news of the rise comes

> out, netizens will definitely be condemning the state, CNPC and Sinopec. At this point, I register an ID and post a comment: "Rise, rise however you want, I don't care. Best if it rises to 50 yuan per litre: it serves you right if you're too poor to drive. Only those with money should be allowed to drive on the roads . . ."
> This sounds like I'm inviting attacks but the aim is to anger netizens and divert the anger and attention on oil prices to me. I would then change my identity several times and start to condemn myself. This will attract more attention. After many people have seen it, they start to attack me directly. Slowly, the content of the whole page has also changed from oil price to what I've said. It is very effective.
>
> **Q** - How big a role do you think this industry plays in guiding public opinion in China?
> **A** - Truthfully speaking, I think the role is quite big. The majority of netizens in China are actually very stupid. Sometimes, if you don't guide them, they really will believe in rumours. [121]

The Chinese government also attempts to monopolize social media and open searching by restricting their citizens' access to certain material. Internet censorship of popular search engines like Google and Yahoo are done through what is known as the Great Firewall of China, a government managed system of content filtration. In addition, the Chinese government backs alternative internet applications like Baidu, the approved search engine in China, Sina Weibo, a Twitter-like service, and Ren Ren, a service that mirrors the functionality of Facebook. Google's adaptation to Chinese law is an ongoing battle worth detailing.

Beginning in 2000, the Chinese government backed an approved search engine Baidu, whose executives catered to government censorship. Shortly after, in September 2002, Google searches within China were banned altogether, completely preventing Chinese citizens from using the tool. In September 2004,

---

[121] Ai Weiwei, "Meet the 50-Cent Party," *New Statesman*, October 2012.
Also published online at http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party.

Google censored antigovernment websites like Greatfire.org, claiming technical difficulties with particular content and "want[ing] to ensure a great user experience." In January 2006, Google launched Google.cn, a Chinese language version of Google meeting the Chinese government's demands for censorship.[122] Google came under attack by open-web supporters many times after this event, but did not change its position.

After this capitulation, Google threatened to close its operation in China in 2010 due to a spate of cyber attacks on its corporate infrastructure.[123] Google complained of surveillance of the online activities of human-rights activists through unauthorized accessing of Google-based e-mail (Gmail) accounts in China and the world along with the theft of intellectual property.[124] Hughes notes that

> Despite the plethora of circumstantial evidence, however, the technical difficulties of attribution make it easy to think of worst-case scenarios under a doctrine of deterrence, such as the triggering of some kind of retaliation by the United States for an attack that appears to come from China but is actually from a group disaffected with that country for one reason or another. It thus seems more likely that any reactions will be confined to traditional measures like diplomatic protests or even economic retaliation and criminal prosecutions, especially if these can encourage self-restraint by damaging China's credibility as a secure place to do business.[125] Google did not decide to leave China, however has continued to proclaim their issues publically about hackers in China.[126]

---

[122] "Google in China Timeline," *International Debates* 8 (2010): 21-23, accessed May 1, 2013, http://theweek.com/article/index/200837/google-in-china-a-timeline.

[123] David Drummond, "A New Approach to China," http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[124] Christopher Hughes, "Google and the Great Firewall," *Survival* 52 (2010): 19-26, accessed on April 9th, 2013, doi:10.1080/00396331003764538.

[125] *Id*.

[126] *Id*.

Google.cn is not a blocked site in China, however Baidu has the upper hand in user activity by a significant margin.

The Chinese government also has effectively replaced all popular social media sites with state-sponsored social media. Twitter and Facebook were blocked by the government following the 2009 riots in Uigher, the capital of

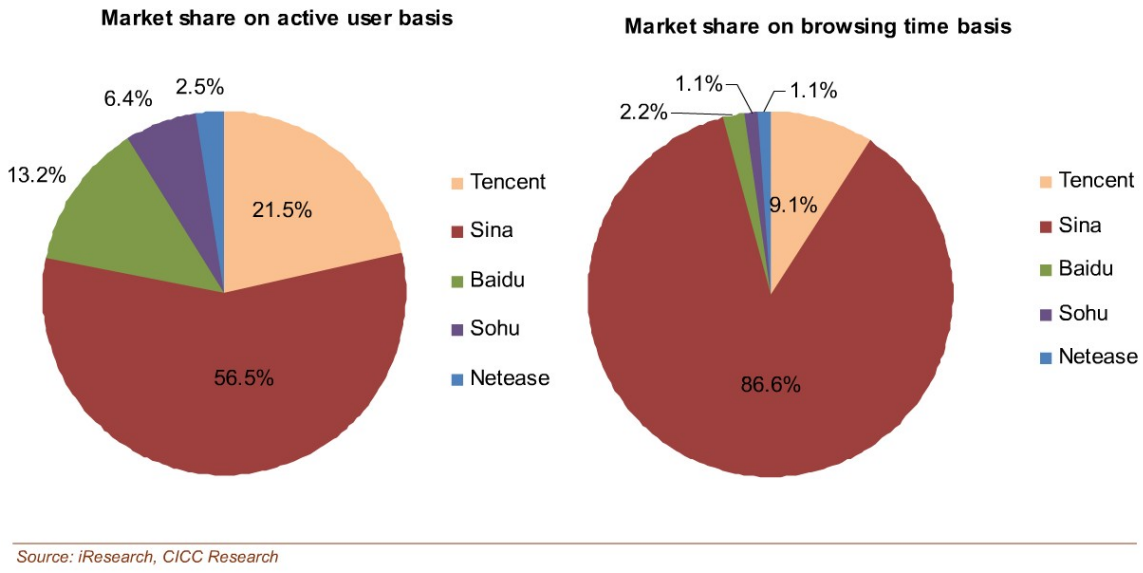

Figure 1.

China's Xinjiang province.[127] Sites like Facebook and Twitter have been shut down by the government because those services are not censored and open the gates for activity deemed damaging to national unification, to unity between the different ethnic groups in China, or to state policy on religion by propagating "feudal beliefs" that endanger social stability.[128] Sina Weibo recently surpassed 400 million users[129] and Renren recently counted over 45 million users.[130] There is

[127] Robin Wauters, "China Blocks Access to Twitter, Facebook After Riots," *Washington Post*, July 7th, 2009, http://articles.washingtonpost.com/2009-07-07/news/36890870_1_facebook-google-apps-google-service.

[128] Christopher Hughes, "Google and the Great Firewall," *Survival* 52 (2010): 19-26, accessed on April 9th, 2013, doi:10.1080/00396331003764538.

[129] Josh Ong, "China's Sina Weibo passes 400m users, acknowledges pressure from rival Tencent's WeChat," *TNW*, November 16, 2012, http://thenextweb.com/asia/2012/11/16/sina-boks-152-million-in-q3-revenue-as-it-faces-tough-competition-from-tencents-wechat/.

increased competition in the social media realm in China with other programs namely Tencent and QQ chat, catching up, however Sina Weibo is consider dominant in popularity and subscribers owning 56% of the micro-blogging market share as illustrated in the graphic above.[131]

While the Great Firewall of China and monopolization of social media govern citizens' activity, self-censorship is ubiquitous as well. Renrou sousou or the "human flesh search engine" and political intimidation incite self-censorship in news media. While both forms are influenced by institutional censorship, they are at times more powerful than government mandate.

The human flesh search engine is not a search engine in the conventional sense, but relies on the collective skills of those who frequent forums and chat rooms to dig up personal information on their targets and then expose this to the media at large in well-publicized name-and-shame campaigns. It's a form of cyber kangaroo court with national consequences and has been used for everything from tracking down a girl who was critical of the government's response to the Sichuan earthquake, to uncovering the identity of a woman who killed a kitten with her high-heel shoe and posted a video of her actions online.[132] The results of activity from the HFS are mixed according to many as witch-hunts for citizens are followed by tales of heroism. In 2008, one HFS episode resulted in the tragic death of an innocent victim. The girlfriend of a young man broke up with him and moved to a different city. In an attempt to locate her, this young

---

[130] Willis Wee, "Renren Has 45 Million Monthly Active Users, Eyes on Mobile," *Techinasia*, August 8th, 2012, http://www.techinasia.com/renren-active-users-45-million/.

[131] "Sina Commands 56% of China's Microblogging Market," accessed May 4th, 2013, http://www.resonancechina.com/2011/03/30/sina-commands-56-of-chinas-microblog-market/.

[132] "People Powered Search Engines: Cyber Witch Hunts or Public Service?," *Beijing Review Forum*, October 23, 2008.

man started an HFS by claiming that he was dying and wanted to see his ex-girlfriend one last time. Out of sympathy to this "dying" man and his last wish,

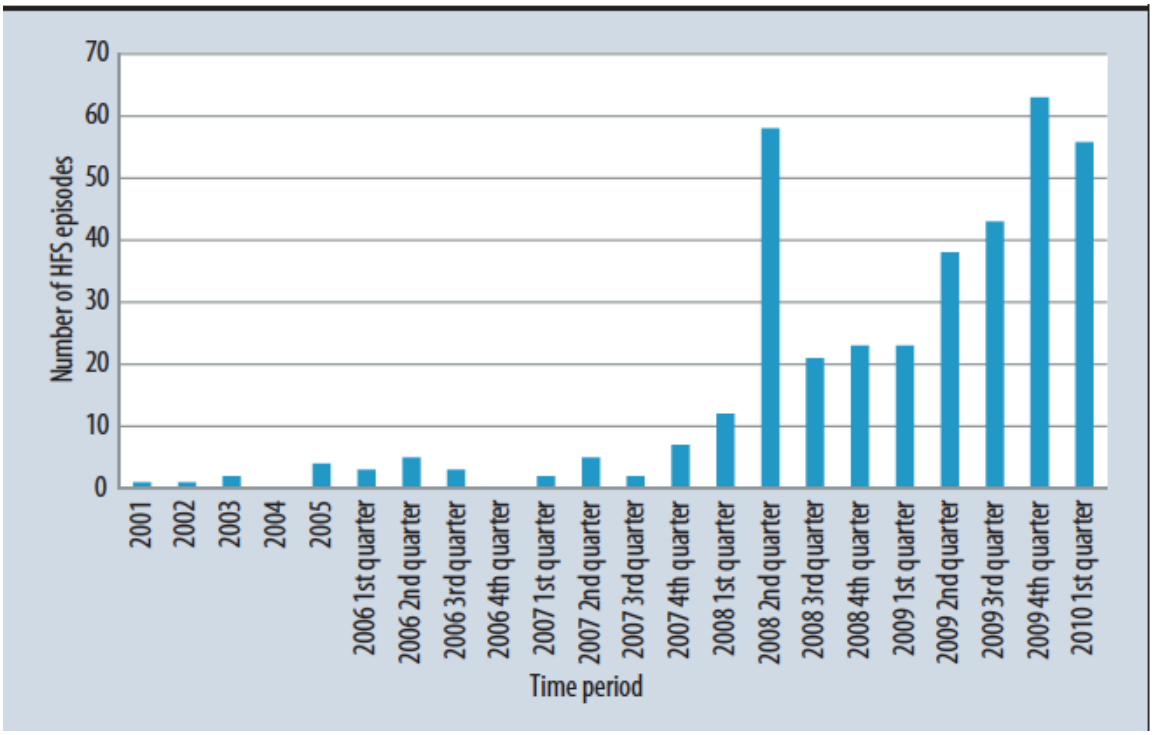

Figure 2. Evolution of HFS episodes quarterly

the HFS community mobilized and successfully found the girl's location. The young man went to meet with her, and after an unsuccessful bid to win her back, killed her with a knife.[133] The HFS also has positive stories, mostly associated with finding missing persons during a national crisis like the earthquake in Sichuan.[134] One aspect of the HFS is its growing popularity in participation. Since 2001, the number of events occurring from the HFS has erupted from an average of one to two per year, to over fifty-five per year in 2010 as seen in Figure 1.[135] While fifty-five events amongst a population of 1.3 billion does not appear to be

[133] Guanpi Lai, "A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge," *Computer Magazine*, August 19 2010, 45-53.

[134] *Id*.

[135] *Id*.

significant, it shows a significant growth in interest amongst Chinese citizens to censor one another's actions to represent the good of the country, the same message passed down from the government with institutional censorship.

Even Hong Kong's news media is affected by self-censorship. Media self-censorship is defined as non-externally compelled acts committed by media organizations aiming to avoid offending power holders such as the government, advertisers, and major business corporations.[136] While the government does not directly censor many of the articles written in Hong Kong, less direct internal pressure is applied to journalist there. Most media organizations in Hong Kong are owned by businesspeople who either have formal political appointments in China or have extensive business interests in the Mainland. Chinese officials also direct occasional warnings and criticisms towards the Hong Kong press, thus setting norms for the media to follow.[137] In 2007 a survey found that 58.5 percent of the Hong Kong journalists interviewed regarded self-censorship as having become more serious than it was ten years ago.

LABOR MOVEMENTS IN CHINA AND SOCIAL MEDIA

China is home to just under 191 million industrial and assembly workers in a labor force of over 795 million people.[138] Manufacturers, miners, utilities and builders accounted for over 45% of China's GDP in 2012. In America, by contrast,

---

[136] Francis L.F. Lee and Joseph Chan, "Organizational Production of Self-Censorship in the Hong Kong Media," *International Journal of Press/Politics*, 14 (2009): 112-133.

[137] *Id*.

[138] "Labor in China: Working Conditions, Wages, and Stress," last modified April 2012, http://factsanddetails.com/china.php?itemid=367.

they contribute less than 20%.[139] In China, all labor union activity is restricted to the ACFTU, or All-China Federation of Trade Unions. ACFTU aims to create an environment to better voice workers' concerns, protect workers' specific interests, fulfill their social functions of protection, construction, participation and education in an all-round way, give prominence to the protective function of trade unions, and unite with and mobilize the broad masses of workers to strive for the realization of the country's socialist modernization.[140] The ACFTU represents 169.94 million workers, with a membership rate of 73.6%.[141] With the government running the union and outlawing alternative unions,[142] the ACFTU cannot represent workers when their interests diverge from state policy. Outside sources like the *Chinese Labour Bulletin* have attempted to bridge the gap between labor members and the government, seeking to represent workers rights at a higher level than the government-run ACFTU.

Labor movement activity has shown marked growth in recent history. According to data from China's Minister of Public Security, in 1997 there were on average 10,000 large-scale collective protests each year. By 2004, the government recorded 74,000 large-scale protests. In 2006, the MPS announced that protests had increased to 87,000, involving over four million workers.[143] This data shows that there is observed growth in labor movement activity and participation. Smith comments that "in China there is now more than enough evidence of

---

[139] "Served in China," *The Economist*, February 23rd, 2013, http://www.economist.com/news/finance-and-economics/21572236-services-are-poised-become-countrys-biggest-sector-served-china.

[140] "A Brief Introduction of the All-China Federation of Trade Unions (ACFTU)," last modified Sept 2007, http://english.acftu.org/template/10002/file.jsp?cid=63&aid=156.

[141] *Id*.

[142] Jerry Harris, Robin Munro, and Michael Zhang, "Defending workers' rights in China: an interview with China Labour Bulletin," *Race Class*, 48 (2007): 83-93.

[143] Brendan Smith, Jeremy Brecher, and Tim Costello, "An Emerging Chinese Labor Movement," *New Labor Forum*, 16 (2007): 83-85, accessed April 2 2013, doi:10.1080/1095760601113431.

worker self-organization outside of official trade union channels to put to rest notions that 'there is no labor movement in China."[144]

There is an understanding that labor movements exist in China, but why they are occurring and at such a high rate are important questions. Barbara Deming of the *LA Times* writes "protests in China have become relatively common over issues such as corruption, pollution, wages, and land grabs that local officials justify in the name of development. People have become increasingly unwilling to accept the relentless speed of urbanization and industrialization and the impact on the environment and health."[145] Howard Friedman of the Huffington Post provides a description of migrant workers in China:

> A significant amount of China's population is trapped in rural poverty or toilsome factory labor with minimal chances of social mobility. As Chinese workers clamor for greater pay and increased rights, factory owners pursue profits by seeking out areas with lower wage pressures. Safe and humane working standards, which laborers fought so hard for in the West, are often absent in developing countries like China, leaving workers susceptible to conditions which Western countries haven't seen on a large scale in generations. Inequalities also exist within the workplace, where migrants often experience lower status, less job stability and lower wages than locals. This struggle between the working class and management/owners is a classic refrain of capitalist societies documented by Marx and Engels.[146]

Some sociological work has been done in China to further understand the dynamics that create an environment as illustrated by Friedman.

Ching Kwan Lee completed an empirical study of two townships in China, Liaoning and Guangdong, to observe how worker communication and

---

[144] *Id*.

[145] Jeffrey Hays, "Protests and Demonstrations in China; The Tensions and Methods Behind Them," *Facts and Details* accessed on October 24, 2013, http://factsanddetails.com/china.php?itemid=305&catid=8.

[146] Howard Steven Friedman, "Is China Posed for Implosion? What would the Communist Manifesto Say?" the Huffington Post, accessed on October 24, 2013, http://www.huffingtonpost.com/howard-steven-friedman/is-china-poised-for-implo_b_690941.html.

protest is organized as well as how the protest groups identify. Lee states "what strikes an outside observer as a homogeneous group confronting common economic predicaments growing out of structural reform is experienced from within the group as fragmented interests, unequal treatment, and mutual suspicion."[147] She goes on to describe labor groups as cellular, commenting that "…a confluence of institutional factors produce the prevailing pattern of cellular activism. State work units provide the physical sites of communication and coordination, organize workers' interests, and define the boundary of the aggrieved community."[148] Based on the context drawn in her book, the usage of cellular labor movements in China suggests that the movements are relatively spontaneous, and do not require much organization to be successful. This is consistent with this thesis's findings regarding the labor movements of Foxconn, Foshan, and Lock factories, as will be seen below.

The most recent and large-scale protest activity that has occurred in China took place at Honda factories in Foshan and Lock. In addition, Foxconn, a leader in electronics assembly and partner with Apple witnessed a large protest in 2012 leading to an internal audit as well as a negotiated wage adjustment and numerous policy changes. There is evidence that these movements began to use differing forms of social media to enhance the effectiveness of their message. Parallel to the incorporation of social media, institutional censorship was still very strong during this time.

In the Foshan and Lock Honda factories in 2010 there were a series of labor protests for wage increases and improved working conditions. Specifically

---

[147] Ching Kwan Lee, *Against the Law: Labor Protests in China's Rustbelt and Sunbelt* (Berkeley: University of California Press: 2007), 84 – 261.

[148] *Id*.

in the Lock factory, workers were looking for a 50% wage increase to roughly $200 a month base salary and were offered a 20% raise initially, to later reject the offer.[149] In Foshan, 2000 workers went on strike for the same cause due to insufficient pay and poor conditions. Management offered the workers a 24% wage increase and the strike ended, however in the process some workers found different ways to express themselves and gain support.

While many workers simply walked out of the Foshan and Lock factories in protest awaiting representation from the ACFTU and their peers, some took to the internet for their cause. The New York Times reported that hours into a strike the workers started posting detailed accounts of the walkout online, spreading word not only among themselves but also to restive and striking workers elsewhere in China. They fired off cellphone text messages urging colleagues to resist pressure from factory bosses. They logged onto a state-controlled Web site — workercn.cn — which is emerging as a digital hub of the Chinese labor movement. And armed with desktop computers, they uploaded video of Honda Lock's security guards roughing up employees.[150] While walkouts were still present during these protests, workers attempted to get the word out not just for their cause, but also in appeal to other factories in China. The disgruntled workers in this southern Chinese city took their cues from earlier groups of Web-literate strikers at other Honda factories, who in mid-May set up Internet forums and made online bulletin board postings about their own

---

[149] David Barboza, "New Strike Threat at a Chinese Honda Parts Plant," *Washington Post*, June 14 2010, accessed December 20 2012, http://www.nytimes.com/2010/06/15/business/global/15strike.html?_r=0.

[150] David Barboza and Keith Bradsher, "In China, Labor Movement Enabled by Technology," *New York Times*, June 16 2010, accessed on December 20, 2012, http://www.nytimes.com/2010/06/17/business/global/17strike.html?pagewanted=all.

battle with the Japanese automaker over wages and working conditions.[151] Recently in China, smartphones and internet services have declined in price, allowing lower income citizens' access to the internet whereas previously it was too expensive. The movement may have stalled if the Chinese government had not made a concerted effort in the last decade to shrink the country's digital divide by lowering the cost of mobile phone and Internet service in this country — a modernization campaign that has given China the world's biggest Internet population (400 million) and allowed even the poorest of the poor to log onto the Internet and air their labor grievances.[152]

With migrant workers and low-income citizens loaded with smartphones, social media protesting and communication began. One method of communication used early on was QQ chat, a simple smartphone enabled chat program available in China that allowed protestors to communicate location, time, and meeting place. Honda's workers set up a QQ group named "Together Is Strength," which not only facilitated media organizations to follow the strike, but also served as a platform for lawyers and labor experts to offer advice.[153] Interviewing a protestor, he explained that he created one the night before the strike, and that had 40 people," said Xiao Lang, one of the two Honda strike leaders in Foshan. Mr. Xiao was fired by Honda soon after leading the walkout. "We discussed all kinds of things on it," he said of the QQ chat room, "such as

---

[151] *Id*.

[152] *Id*.

[153] Jennifer Cheung, "Chinese Workers Gain Strength in Cyberspace," *Forbes Magazine*, June 1 2011, accessed on December 23 2012, http://www.forbes.com/sites/jennifercheung/2011/06/01/chinese-workers-gain-strength-in-cyberspace/.

when to meet, when to walk out and how much pay we want."[154] QQ allowed protestors a tool to organize, which assisted in leading over 2000 protesters in Foshan, but it wasn't the only form of online communication used.

Protestors also posted videos and pictures of acts of aggression towards their peers as a method of outing the Honda management's attempts to stop the protest. Labor activists have been exposing the harsh working conditions in Chinese factories by smuggling cellphone images and video out of coastal factories and posting documents showing labor law violations on the Web. New and notable is that these formerly covert activities have become open and pervasive. The target sources for posting such pictures and videos are popular Chinese web locations www.youku.com, 56.com, and the dominant search engine Baidu.com, all censored by the Chinese government but did catch some foreign media attention before being scaled back.[155] While it is well documented that labor unrest has been plentiful in the Chinese auto industry, electronics leader Foxconn has seen its fair share of labor dispute as well.

In September of 2012, a riot broke out at the Foxconn electronics factory in Taiyuan, in Shanxi Province, in which 5000 police officers were called to quiet the outburst. While many accounts of the riot differed, an official statement from the supplier said that 40 people were hospitalized and many were arrested during the riot, which lasted several hours after it broke out late Sunday night. The company said the dispute appeared "not to have been work-related," which conflicts with unconfirmed reports on Chinese social media sites that claim the

---

[154] David Barboza and Keith Bradsher, "In China, Labor Movement Enabled by Technology," *New York Times*, June 16 2010, accessed on December 20, 2012, http://www.nytimes.com/2010/06/17/business/global/17strike.html?pagewanted=all.

[155] *Id.*

melee began after a security guards beat a worker.[156] Analysts say workers unrest in China has grown more common because workers are more aware of their rights, and yet have few outlets to challenge or negotiate with their employers. When they do, though, the results can be ugly and, because of social media and the Web, almost instantly transmitted to the world, targeted mostly at Western bloggers and news media, in their rawest and most unfiltered form.[157] The breadth of the situation is larger than it appears as Foxconn employs over 1.1 million workers worldwide and most of the rioting workers claimed they heard what had occurred at other factories in China and wanted the same concessions. While the factory representatives downplayed the incident, a social media post from a factory worker claimed a large number of workers were moved to Taiyuan to make iPhone 5 in a rush. The security personnel at the factory fought with a worker from Shandong Province in which he dragged him to a van and beat him up. The victim's co-workers from Shandong sought revenge, and workers from Henan Province became involved too, and the situation devolved into chaos where workers chased down security guards and beat them up.[158]

In addition to some media reporting on the riot, some Western bloggers and writers were attempting to gather pictures and video before the material was censored to broadcast in an uncensored place. Richard Lai, a senior associate editor at Engadget, a technology blog, was monitoring posts on Chinese social media sites mostly from Sina Weibo. Mr. Lai reported that several people said

---

[156] Jennifer Preston, "Chinese Social Media Accounts Clash With Official Reports on Riot at Foxconn," *The New York Times*, September 24th, 2012, http://thelede.blogs.nytimes.com/2012/09/24/chinese-social-media-accounts-clash-with-official-reports-on-riot-at-foxconn-factory/.

[157] David Barboza and Keith Bradsher, "Riot at Foxconn Factory Underscores Rift in China," *The New York Times*, September 24, 2013, http://www.nytimes.com/2012/09/25/business/global/foxconn-riot-underscores-labor-rift-in-china.html.

[158] *Id*.

the disturbance started after a worker was beaten. Mr. Lai also published photos of what appeared to be damage resulting from the riot that was shared on social sites; many of the photos were soon removed from the Web. "Sina Weibo is already censoring the Foxconn riot pics, apparently. Ugh. @richardlai."[159] The method that has worked to some extent is attempting to distribute material to censored sites with the hope that bloggers and activist groups outside of China redistribute before censorship occurs.

SOCIAL MEDIA SUCCESS?

Much has been documented on the tactics used by protestors and rioters in Foshan, Lock, and Foxconn in an attempt to change company policies, increase wages and conditions, as well as balance employees' work and personal life. Separate from walkouts, social media tools namely QQ chat, workerscn.cn, youku.com, 56.com, and Baidu are a few of the methods mentioned in this thesis. In addition, communication directly through the ACFTU, the acting labor movement body in China, has been attempted to gain ground in the multitude of disputes in the past few years.

QQ chat was mentioned throughout a number of sources as a method used by rioters to communicate amongst themselves and the media on the events as they unfolded. Numerous rooms or chats were started to generate buzz as to the priorities of each movement and what change was proposed. While a popular method at the time, not all observers felt it was a successful means of

[159] Jennifer Preston, "Chinese Social Media Accounts Clash With Official Reports on Riot at Foxconn," *The New York Times*, September 24th, 2012, http://thelede.blogs.nytimes.com/2012/09/24/chinese-social-media-accounts-clash-with-official-reports-on-riot-at-foxconn-factory/.

communication as it was soon infiltrated by Honda Lock officials and government security agents, forcing some to move to alternative sites.

> We're not using QQ any more, said one strike leader here. There were company spies that got in. So now we're using cellphones more. QQ offers no protection from eavesdropping by the Chinese authorities, and it is just as well they stopped using it, said Rebecca MacKinnon, a China specialist and fellow at the Center for Information Technology Policy at Princeton University. QQ is not secure. You might as well be sharing your information with the Public Security Bureau.[160]

In addition to QQ chat not being secure, workercn.cn, noted as a popular site for laborers to voice their concerns, is controlled by the Chinese government and 56.com is owned by Renren[161], another company known for significant censorship in China. Youku.com, the most popular video-sharing site, was warned by the Chinese government for walking the line of law in China with its content as it did not have a SARFT (State Administer of Radio, Film, and Television) approval until 2008 when the government threatened to remove the site. The approval ensures that the content on Youku.com is operating at a level of censorship deemed acceptable by the government.[162] Baidu beat out Google for the #1 search engine due to Google's lack of compliance with Chinese censorship demands. Furthermore, documents[163] expose Baidu as one of the most censored outlets in China, while also being one of the most popular at 80 million hits a day

---

[160] David Barboza and Keith Bradsher, "In China, Labor Movement Enabled by Technology," *New York Times*, June 16 2010, accessed on December 20, 2012, http://www.nytimes.com/2010/06/17/business/global/17strike.html?pagewanted=all..

[161] Jiang Chang, "56.com: The Double-Edged Sword For Renren," *Seeking Alpha*, September 28th, 2011, http://seekingalpha.com/article/296478-56-com-the-double-edged-sword-for-renren.

[162] Betsy Schiffman, "Youku Gets Chinese Government's Blessing," *Wired*, July 10m 2008, http://www.wired.com/business/2008/07/youku-gets-chin/.

[163] "Baidu Censorship Documents Leaked," visited on October 1, 2013, http://blog.webcertain.com/baidu-censorship-documents-leaked/08/05/2009/.

from cell phones.[164] As one can see, Chinese censorship is not limited to internet websites, but includes mobile applications, and social media programs covering the entire spectrum of electronic communication found popular in these labor movements. While these web pages and media outlets are ways in which protestors attempted to get the word out, the other side of this argument is the relative silence of social media.

Concessions were triggered in the Chinese labor disputes not through social media but by way of walkouts in Chinese factories accompanied by NGOs and western media pressuring the parent company, Apple, to take action. On January 6th, "This American Life" ran an hour-long feature on the horrendous working conditions at Foxconn. Their investigation helped get the media circus cued up. Later in January, the *Times* ran one of their in-depth, Pulitzer-eyeing reports that painted a grim-if not desperate picture of the iPain behind iPad. These reports led Apple to join the Fair Labor Association, change in factory policy occurred shortly afterwards.[165]

> You would think that an Apple Spring uprising would have erupted on Facebook and Twitter, encouraging boycotts and demanding change. You'd expect flash mobs in front of those crystal palaces otherwise known as Apple stores. After all, the cultural moment is right for outrage. Punishing a company for its distant but very real practices is a Hollywood protest story that taps into the latent, populist, hostility toward globalization and our natural sympathy for the underclass. And all of it is amplified by the Occupy Wall Street movement, which has sensitized us to examples of the powerful taking advantage of the powerless.[166]

---

[164] Josh Ong, "Baidu aggressively investing in mobile and the cloud as it tops 80m daily mobile search users." *Thenextweb.com*, February 5, 2013, http://thenextweb.com/asia/2013/02/05/baidu-aggressively-investing-in-mobile-and-the-cloud-as-it-tops-80m-daily-mobile-search-users/.
"Baidu's Internal Monitoring and Censorship Document Leaked," last visited September 20, 2013, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/.

[165] Adam Hanft, "Foxconn and the Curious Silence of Social Media," *Hanft Unlimited*, March 3, 2012, http://www.huffingtonpost.com/adam-hanft/apple-foxconn-china_b_1392339.html.

[166] *Id.*

Adam Hanft, political columnist, claims that social media was relatively dead during the debate, "most Americans barely heard of the events, and traditional methods of social change prevailed over social media."[167]

Some writers have concluded that the result of these protests was a success and important concessions were made using social media. Taken from an article on NPR:

> "Over the summer, a rash of suicides and strikes hit factories in southern China as workers protested against labor conditions. Rather than cracking down, factory bosses have responded to the protests by increasing salaries and improving working conditions. "This is all happening, firstly, because it is a new, younger generation of migrant workers, who won't accept such bad conditions," he says. "Secondly, there's a shortage of workers, so they know they have more leverage. And thirdly, cell phones and the Internet mean they know more about the outside world, and are better able to organize as well."[168]

The demands of the workers in Foshan specifically were for an 89% increase in wage, that number signifying a match of other Honda workers wages in China, specifically workers in the Nanhai factory. After the protest ended and workers returned to their duties, they did so on a 24% wage increase.[169] The workers were making 900 yuan a month, equal to $132 US dollars. They demanded an increase to 1700 yuan, equating to $249.28 and ended up with $163.68, which is $85.60 less than the neighboring Honda factory.

The impact of social media on China's various labor movements is affected by the two forms of censorship described in this thesis. Institutional censorship is embedded in Chinese culture, facilitated by the Chinese

---

[167] *Id*.

[168] Rob Gifford, "Momentum Builds Behind Chinese Workers' Protests," *NPR*, September 24, 2010, http://www.npr.org/templates/story/story.php?storyId=130078240.

[169] John Chan, "Honda Lock strike in China continues as industrial unrest spreads," *World Socialist Web Site*, June 12, 2010, http://www.wsws.org/en/articles/2010/06/hond-j12.html.

government, and legalized to the extent that a strict system of checks and balances is in place. Forms of direct monitoring exist in almost every facet of Chinese citizens' internet experience, from website and content blocking, to the 50-cent party infiltration, a relatively tacit yet effective method of censorship. As for self-censorship, the human flesh search engine was create by Chinese citizens as a supplement to the government's behavior, casting out rogue individuals whose actions are deemed unacceptable by the masses and chastising them publically for what is considered the greater good. Political intimidation has imposed fear on citizens via the government's strict policies on acting against the "greater good of the Chinese state;" outcasts like Ai Wei Wei have been banished from China for their beliefs.

Examining the Foshan, Lock, and Foxconn labor protests shows that as Chinese workers gained an understanding of the tools available to win their concessions from their employers, infiltration, censorship, and the lack of representation in the government-run ACFTU sharply limited media attention in Western states, even though limited wage gains were made. While there is no doubt that labor disputes will continue in China due to limited victories in particular factories, without a significant change to the censorship policies followed by government and corporate representatives, social media will continue to be a low impact tool, monitored and censored with few or no results.

CHAPTER 6: CONCLUSION

A wide array of data has been shared in this thesis to answer the question posed initially: with the high level of investment in data mining and data censorship in the U.S. and China, has social media been an effective tool for social protest and activist activity in these countries? This argument began with an example during the Arab Spring movement in the Middle East, concluding that occupy-related tactics were much more successful than social media as an agent for change. Next, a literature review outlined supporters and opponents of the view that social media is an effective tool in social protest. Supporters, namely Clay Shirky and Rebecca Mackinnon, praised social media for its speedy response time and Mackinnon specifically notes that Chinese protestors have found methods around the 'Great Firewall" seemingly painting the picture of Chinese censorship as weak compared to its perception. As for opposing arguments, Malcolm Gladwell coined the term *Slacktivism* for the notion that activism via social media is close to meaningless and that real social change is brought about through high-risk, well-organized, committed groups whose ideals are in alignment. Evgeny Morozov's main thesis is that a sense of security and privacy are illusions, coining the term 'cyber-utopianism,' referring to the view that the internet is liberating due to its lack of *evident* controls. In the third chapter, the methods of research are outlined for the U.S. and China. Some methods used are Supreme Court cases and Chinese electronic policies to emphasize the legal framework behind data usage. The terms of service for Facebook and Twitter are broken down as well as incorporating online journals, web articles, FoIA requested documents, and definitions of pertinent terms.

Chapters four and five contain the bulk of the data on the U.S. and China as the legal history of each location are expanded to included the specific court cases and documents used to spell out the conditions of legality for data usage. The majority of sources used for the U.S. example are unclassified DHS documents on surveillance activities following the Occupy Wall Street movement. The data for China is an expansion on institutional and self-censorship tactics namely abundant government internet censorship, infiltration via the 50-cent party, followed by labor disputes at Honda's Foshan and Lock factory as well as Foxconn electronics.

Based on the data discovered during the research phase of this thesis, my conclusion of the posed question is that social media is not only ineffective for social movements and activist activity in the United States and China, it negatively impacts the desired outcome in some examples. The state of the Occupy Wall Street movement, pending any sort of resurgence, shows that the lack of organization, mixed with an unclear agenda, and rampant use of the internet to organize has been a major downfall for participants. The protest activity of the movement is monitored regularly, evident in police presence before the protesting begins. With the lack of media attention in the last nine months, the movement appears to have lost its initial steam. As for labor protests in China, they will continue to attract attention not because of social media, but mainly because of organizations like the *China Labour Bulletin* and Human Rights Watch. As argued by columnist Adam Hanft, the social media presence in these labor disputes is almost non-existent due to censorship; media exposure of Chinese labor issues has been taken on by advocacy groups, not the protestors.

AN ALTERNATIVE: GERMAN *RASTERFAHDUNG*

Unlike the U.S. or China, some countries have found a less extreme approach to data mining. The U.S. position on data mining has been straightforward; constitutional law and criminal procedure leave data mining, whether subject-based or pattern-based, largely unregulated.[170] Evidence of this was found in US v. Miller and Smith v. Maryland, which concluded that the Fourth Amendment is inapplicable to stored data in the control of third parties and to any aspect of telecommunications that is not "content" of a telephone conversation.[171] A majority of online content is controlled by third parties (almost all social media), making this data is fair game and 'public.'

The German government has had numerous court cases on data mining as well, otherwise known as *Rasterfahndung*, or data screening. The laws however, have been molded by court cases and legislation which have changed to meet the evolving times (the constitution has been amended as recently as 1990), differing drastically from U.S. laws. For data screening to pass constitutional muster in Germany a 'concrete danger' must be present, defined as "when necessary to defend against a present danger (*gegenwärtige Gefahr*) to the existence or the security of the federation or a state, or the body, life, or freedom of a person."[172]

---

[170] Paul M. Schwartz, "Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, The State, and New Technology," 53 Wm. & Mary L. Rev. 351 (2011), http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3405&context=wmlr.

[171] Paul M. Schwartz, "German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance," 54 Hastings L.J 751, 764-65 (2003), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=425521.

[172] Polizeigesetz des Landes Nordrhein-Westfalen (North Rhine-Westphalia Police Statute), 10 Gesetz-Und Verordnungsblatt Fur Das Land Nordrhein Westfalen 70, § 31 (1990).

In U.S. courts, data mining can be justified through a general threat of terrorism[173], not specific, case-by-case instances.

Another stipulation of German data screening is that the act of screening a citizen's information must not violate the right to self-determination as defined as a citizens right to a private sphere in which one is to be free to shape her life, a right to one's spoken word, and, of particular relevance in the *Data Screening* case, a right to informational self-determination.[174] To elaborate on this topic, the German constitutional court raised issues concerning the threat of modern means of surveillance to an individual's underlying communicative ability, noting that a person who is unable with sufficient security to assess the knowledge of information that concerns him in certain sectors of his social environment, who cannot to some extent estimate the knowledge of possible communication partners, is at risk.[175] Essentially, self-determination safeguards citizens from data screening in which they are ignorant of their security and cannot know how their information is being used.

Lastly, coming from a German Constitutional Court decision post-September 11th in conjunction with the German 'concrete danger' definition, a German justice noted "foreign political areas of tension that terrorists could use an occasion for attacks always exist" and this state of affairs "can last a long time."[176] As a result, the Constitutional Court concluded:

> As a practical manner, it is never out of the question that terrorist actions can hit Germany or can be prepared there. A general threat situation, which has existed practically without break since September 11, 2001, that

---

[173] *Id.* Schwartz.

[174] Das *Bundesverfassungsgericht Dec. 15, 1963 BVerfGE 1, http://www.servat.unibe.ch/dfr/bv001014.html*.

[175] *Id.* BVerfGE 70.

[176] BVerfGE 320, para 147. At 364.

> is for more than four years now, or foreign tensions are not sufficient for the ordering of data screening.[177]

The German court determined that while there is always a threat of terrorism, allowing what would normally be an unconstitutional action proceed without 'concrete danger,' would not be justified.[178] The German Constitutional Court has embraced a "new constitutionalism", demonstrated by its strong engagement in developing and shaping constitutional norms to respond to the threat of technological developments to civil liberties, as opposed to adapting current conditions to an out-of-date text, resistant to change.[179]

CLOSING

While much has been uncovered in recent history on data mining and censorship in the U.S. and China, much more is to come as the debate on constitutionality has been as active as ever. Recent events such as Julian Assange's WikiLeaks website and Edward Snowden's public outing of the NSA, are the beginning of a long battle for citizens' digital privacy. There are many predictions of what will occur on this topic in the future from underground, alternative internet sources, extreme governmental hacking activity, privatization of the internet, to Eric Schmidt's (CEO of Google) "web 3.0 automation" concept written about in his book *The New Digital Age: Reshaping the*

---

[177] *Id*.

[178] While too long to explain here, Schwartz continues to describe how the German Constitutional system differs from the U.S. Constitution. He notes post-war constitutions are typically far more extensive and specific than a founding document from the eighteenth century, post-war E.U. constitutions typically contain more detailed rights provisions than the U.S. Constitution, and post-war constitutions of Europe typically assign a central role in developing the higher law to a constitutional court that is separate from the rest of the court system. See Schwartz p. 377-378.

[179] *Id*. Schwartz 378.

Future of People, Nations and Business.[180] While this topic seems to be a 'wait and see' situation, one prediction that is not getting much attention is the lack of opt-out possibilities.

Currently in social media all new users need to agree to the ToS or terms of service before using the program. As mention previously in this thesis, these privacy statements are cryptic and riddled with terms most users would not agree to if understood. While social media companies have a right to state their terms, one cannot use these programs without agreeing to third party ownership of personal information. The only way to dodge these clauses is abstinence, with a lack of any alternative. This creates an online environment of entrapment for users as they are fooled into believing their data is safe, even in a private writing area like a blog.

For decades men and women of the United States have fought for rights to avoid enslavement, voting, equality, and liberty. In the current era, citizens are voluntarily giving their rights away with regard to privacy for the sole purpose of staying connected with social media. Tempting as social media is to satisfy our natural urge to stay connected with the world, there are privacy sacrifices being made in exchange. It is essential to be an informed citizen regarding one's personal data, and while privacy on the internet is a trending conversation thanks to Edward Snowden, the conversation must continue and evolve for change to occur.

---

[180] Eric Schmidt, *The New Digital Age: Reshaping the Future of People, Nations and Business (New York:* Knopf 2013).

BIBLIOGRAPHY

ACFTU. "A Brief Introduction of the All-China Federation of Trade Unions (ACFTU)," last modified Sept 2007. http://english.acftu.org/template/10002/file.jsp?cid=63&aid=156.

Barboza, David and Bradsher, Keith. "In China, Labor Movement Enabled by Technology." *New York Times*, June 16 2010. accessed on December 20, 2012. http://www.nytimes.com/2010/06/17/business/global/17strike.html?pagewanted=all.

Barboza, David and Bradsher, Keith. "Riot at Foxconn Factory Underscores Rift in China." *The New York Times*, September 24, 2013. http://www.nytimes.com/2012/09/25/business/global/foxconn-riot-underscores-labor-rift-in-china.html.

Barboza, David."New Strike Threat at a Chinese Honda Parts Plant." *Washington Post*, June 14 2010. http://www.nytimes.com/2010/06/15/business/global/15strike.html?_r=0.

Barrett, Devlin. "'Tripwires' Can Spot Would-Be Bombers." *The Washington Post,* April 15, 2013. http://online.wsj.com/article/SB10001424127887324345804578425483373542340.html.

Blood, Rebecca. "Weblogs: A History and Perspective." rebeccablood.net. Sept 7, 2000. http://www.rebeccablood.net/essays/weblog_history.html.

BVerfGE 320, para 147. At 364.

Chan, John. "Honda Lock strike in China continues as industrial unrest spreads." *World Socialist Web Site*, June 12, 2010. http://www.wsws.org/en/articles/2010/06/hond-j12.html.

Chang, Jiang. "56.com: The Double-Edged Sword For Renren." *Seeking Alpha*, September 28th, 2011. http://seekingalpha.com/article/296478-56-com-the-double-edged-sword-for-renren.

Cheung, Jennifer. "Chinese Workers Gain Strength in Cyberspace." *Forbes Magazine*, June 1 2011. accessed on December 23 2012. http://www.forbes.com/sites/jennifercheung/2011/06/01/chinese-workers-gain-strength-in-cyberspace/.

China Digital Times."Baidu's Internal Monitoring and Censorship Document Leaked." last visited September 20, 2013.

http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/.

Chinese Government Website. "The Internet in China," created June 8th 2010. http://english.gov.cn/2010-06/08/content_1622956_6.htm.

Das *Bundesverfassungsgericht Dec. 15, 1963 BVerfGE 1*, http://www.servat.unibe.ch/dfr/bv001014.html.

Department of Homeland Security U.S. Customers and Border Protection. *Significant Incident Report*, reported on January 1, 2012.

Department of Homeland Security. *FOIA Transmissions*, report 5 November 2011.

Dorling, Philip. "Media is a Double Edged Sword." *Canberra Times,* January 29, 2011.

Drummond, David. "A New Approach to China." http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Economist. "Served in China," *The Economist*, February 23rd, 2013. http://www.economist.com/news/finance-and-economics/21572236-services-are-poised-become-countrys-biggest-sector-served-china.

Esdandiari, Golnaz. "Twitter Devolution." *Foreign Affairs*, June 7 2010. http://www.foreignpolicy.com/articles/2010/06/07/the_twitter_revolution_that_wasnt.

Facts and Details."Labor in China: Working Conditions, Wages, and Stress." last modified April 2012, http://factsanddetails.com/china.php?itemid=367.

Federal Bureau of Investigation Anchorage. *Field Report Anchorage*, report from 11/3/2011.

Federal Bureau of Investigation Anchorage. *Field Report Anchorage*, report from 28 November 2011.

Federal Bureau of Investigation Indianapolis. *Situational Information Report*, report from 9/15/2011.

Federal Bureau of Investigation Jacksonville. *Field Report Jacksonville*, report from 19 October 2011.

Federal Bureau of Investigation New York. *Field Report New York*, report for 8/22/2011.

Federal Bureau of Investigation Richmond. *Situational Information Report*, report from 13 October 2011.

Forum. "People Powered Search Engines: Cyber Witch Hunts or Public Service?," *Beijing Review Forum*, October 23, 2008.

Free Speech Debate,"China's human flesh search engines." published July 3, 2012. http://freespeechdebate.com/en/discuss/chinas-human-flesh-search-engines/.

Friedman, Howard Steven."Is China Posed for Implosion? What would the Communist Manifesto Say?." *Huffington Post*, accessed on October 24, 2013. http://www.huffingtonpost.com/howard-steven-friedman/is-china-poised-for-implo_b_690941.html.

Gifford, Rob. "Momentum Builds Behind Chinese Workers' Protests." *NPR*, September 24, 2010. http://www.npr.org/templates/story/story.php?storyId=130078240.

Gladwell, Malcolm. "Small Change." *New Yorker*, Oct 4 2010. www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

Google. "Control Permissions." last modified February 15th, 2013. http://support.google.com/blogger/bin/answer.py?hl=en&answer=42673.

Google. "Google Privacy Policy." last modified July 27, 2012. http://www.google.com/policies/privacy/?hl=en.

Hanft, Adam. "Foxconn and the Curious Silence of Social Media." *Hanft Unlimited*, March 3, 2012, http://www.huffingtonpost.com/adam-hanft/apple-foxconn-china_b_1392339.html.

Harris, Jerry, Munro, Robin, and Zhang, Michael. "Defending workers' rights in China: an interview with China Labour Bulletin." *Race Class*, 48:2007.

Hays, Jeffrey. "Protests and Demonstrations in China; The Tensions and Methods Behind Them." *Facts and Details,* accessed on October 24, 2013. http://factsanddetails.com/china.php?itemid=305&catid=8.

Hughes, Christopher. "Google and the Great Firewall," *Survival*, 52:2010. accessed on April 9th, 2013, doi:10.1080/00396331003764538.

Jones, Thai. "As Occupy Wall Street Fades, Powerful Ideas May Live On." *Bloomberg.com*, September 21st, 2012. http://www.bloomberg.com/news/2012-09-21/as-occupy-wall-street-fades-powerful-ideas-may-live-on.html.

Joseph, Sarah. "Social Media, Political Change, and Human Rights." Law Review, Boston College, 2012, Vol. 35 Issue 1.

Justice Online. "FBI Documents Reveal Secret Nationwide Occupy Monitoring." last modified December 22nd, 2012. http://www.justiceonline.org/commentary/fbi-files-ows.html.

Katz v. United States, 389 U.S. 347 1967.

Kessler, Sarah. "Why Social Media is Reinventing Activism." *Mashable* (Oct 9, 2010). mashable.com/2010/10/09/social-media-activism.

Lai, Guanpi."A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge," *Computer Magazine*, August 19 2010.

Lee, Ching Kwan. "Against the Law: Labor Protests in China's Rustbelt and Sunbelt." *Berkeley: University of California Press*: 2007.

Lee, Francis L.F. and Chan, Joseph. "Organizational Production of Self-Censorship in the Hong Kong Media," *International Journal of Press/Politics*, 14:2009.

Lehman, Lee, Xu, "The Temporary Regulation for the Management of Computer Information Network International Connection," *Lehman Law*, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html.

LexisNexis. "LexisNexis Accurint Government Sample Reports." https://learn.lexisnexis.com/lexisnexis/user_training.aspx?solution=%23gsr.

MacKinnon, Rebecca. "The (not-so-great) Firewall of China." *Toronto Star* April 28, 2012.

Mohammed, Arshad, and Goo, Sara Kehaulani. "Government Increasingly Turning to Data Mining." *The Washington Post*, June 15th, 2006. www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Foreign Affairs, 2011.

New Scientist. "Was the Arab Spring really a Facebook revolution?." Published April 13th, 2012. http://www.newscientist.com/article/mg21428596.400-was-the-arab-spring-really-a-facebook-revolution.html.

Occupy Wall Street. "#Howto Occupy." http://howtooccupy.org/.

Occupy Wall Street. "#Occupy Wall Street NYC General Assembly." http://www.nycga.net/events/.

Occupy Wall Street. "Occupy Archive." http://occupyarchive.org/about.

Occupy Wall Street. "Occupy Chat." http://occupywallst.org/chat/.

Occupy Wall Street. "Occupy Forum." http://occupywallst.org/forum/.

Occupy Wall Street. "Occupy Infotent." http://occupywallst.org/infotent.

Occupy Wall Street. "Occupy Map." http://occupywallst.org/attendees/.

Occupy Wall Street. "Occupy Streams." http://occupystreams.org/.

Occupy Wall Street. "Occupy Wall Street Facebook Site." https://www.facebook.com/OccupyWallSt1?fref=ts.

Occupy Wall Street. "Occupy Wall Street: The Bloom is Fading." November 7th, 2011. http://www.economist.com/blogs/democracyinamerica/2011/11/occupy-wall-street.

Occupy Wall Street. "Occupy Wall Street." last modified April 14th, 2013. http://occupywallst.org/.

Ong, Josh. "Baidu aggressively investing in mobile and the cloud as it tops 80m daily mobile search users." *Thenextweb.com*, February 5, 2013. http://thenextweb.com/asia/2013/02/05/baidu-aggressively-investing-in-mobile-and-the-cloud-as-it-tops-80m-daily-mobile-search-users/.

Ong, Josh. "China's Sina Weibo passes 400m users, acknowledges pressure from rival Tencent's WeChat," *TNW*, November 16, 2012. http://thenextweb.com/asia/2012/11/16/sina-boks-152-million-in-q3-revenue-as-it-faces-tough-competition-from-tencents-wechat/.

Pfeifle, Mark. "The Nobel Peace Prize for Twitter?." *CSMonitor.com*, July 6th 2009. http://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html.

Polizeigesetz des Landes Nordrhein-Westfalen (North Rhine-Westphalia Police Statute), 10 Gesetz-Und Verordnungsblatt Fur Das Land Nordrhein Westfalen 70, § 31 (1990).

Preston, Jennifer. "Chinese Social Media Accounts Clash With Official Reports on Riot at Foxconn." *The New York Times*, September 24th, 2012. http://thelede.blogs.nytimes.com/2012/09/24/chinese-social-media-accounts-clash-with-official-reports-on-riot-at-foxconn-factory/.

Resonancechina. "Sina Commands 56% of China's Microblogging Market," accessed May 4th, 2013. http://www.resonancechina.com/2011/03/30/sina-commands-56-of-chinas-microblog-market/.

Salem News. "Homeland Security Documents Show Massive Nationwide Monitoring of Occupy Movement." *Salem News,* May 4th, 2012. http://www.justiceonline.org/commentary/dhs-releases-more-documents.html.

Salem-News. "Homeland Security Documents Show Massive Nationwide Monitoring of Occupy Movement – This set of released materials reveals intense involvement by the DHS National Operations Center (NOC) in these activities." *Salem-News*, May 4th 2012. http://www.justiceonline.org/commentary/dhs-releases-more-documents.html.

Schiffman, Betsy. "Youku Gets Chinese Government's Blessing." *Wired*, July 10m 2008. http://www.wired.com/business/2008/07/youku-gets-chin/.

Schmidt, Eric. *The New Digital Age: Reshaping the Future of People, Nations and Business* New York, Knopf 2013.

Schwartz, Paul M.. "German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance." 54 Hastings L.J 2003. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=425521.

Schwartz, Paul M.. "Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, The State, and New Technology." Wm. & Mary L. Rev. 351:2011. http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3405&context=wmlr.

Search Engine Journal. "The Growth of Social Media: An Infographic." Published August 30th, 2011. http://www.searchenginejournal.com/the-growth-of-social-media-an-infographic/32788/.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs*, Jan/Feb 2011, Vol. 90 Issue 1, p28-41.

Smith v. Maryland, 442 U.S. 735 (1979).

Smith, Brendan, Brecher, Jeremy, and Costello, Tim. "An Emerging Chinese Labor Movement." *New Labor Forum*, 16:2007 April 2 2013. doi:10.1080/1095760601113431.

Sullivan, Andrew. "The Revolution will be Twittered." *The Atlantic*, June 13th 2009.

Tam, Donna. "Facebook by the numbers: 1.06 billion monthly active users." *CNet*, January 30, 2013. http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users.

The Week. "Google in China Timeline." *International Debates,* 8:2010 accessed May 1, 2013, http://theweek.com/article/index/200837/google-in-china-a-timeline.

Twitter. "Twitter Terms of Service." last modified June 25th, 2012. https://twitter.com/tos.

Twitter. "Twitter Transparency Report," last modified July 2, 2012. http://blog.twitter.com/2012/07/twitter-transparency-report.html.

Twitter. "U.S. Twitter Transparency Report." last modified January, 2013. https://transparency.twitter.com/information-requests/US.

U.S. Const. amend. IV.

Unet. "Unet: Social Network." http://www.unet.net/.

United States v. Miller, 425 U.S. 435 (1976).

US Constitution. "FISA Amendment 2008." last modified July 8th, 2008. http://www.govtrack.us/congress/bills/110/hr6304/text.

US Supreme Court Center. "US Supreme Court Center." http://supreme.justia.com/cases/federal/us/425/435.

US Supreme Court Center."US Supreme Court Center." http://supreme.justia.com/cases/federal/us/389/347/case.html.

US Supreme Court Center."US Supreme Court Center." http://supreme.justia.com/cases/federal/us/442/735/case.html.

Wauters, Robin. "China Blocks Access to Twitter, Facebook After Riots." *Washington Post*, July 7th, 2009. http://articles.washingtonpost.com/2009-07-07/news/36890870_1_facebook-google-apps-google-service.

Webcertain."Baidu Censorship Documents Leaked." visited on October 1, 2013. http://blog.webcertain.com/baidu-censorship-documents-leaked/08/05/2009/.

Wee, Willis "Renren Has 45 Million Monthly Active Users, Eyes on Mobile," *Techinasia*, August 8th, 2012. http://www.techinasia.com/renren-active-users-45-million/.

Weiwei, Ai. "Meet the 50-Cent Party." *New Statesman*, October 2012.